(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001 年6 月7 日 (07.06.2001)

PCT

(10) 国際公開番号
WO 01/41356 A1

(51) 国際特許分類[7]: H04L 9/10, G06F 12/14, G10K 15/02, G06F 13/00

(21) 国際出願番号: PCT/JP00/08544

(22) 国際出願日: 2000 年12 月1 日 (01.12.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/343389 1999 年12 月2 日 (02.12.1999) JP

(71) 出願人 (米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP). 株式会社 ピーエフユー (PFU LIMITED) [JP/JP]; 〒929-1125 石川県河北郡宇ノ気町字宇野気ヌ98番地の2 Ishikawa (JP). 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP). 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP). 日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 Tokyo (JP).

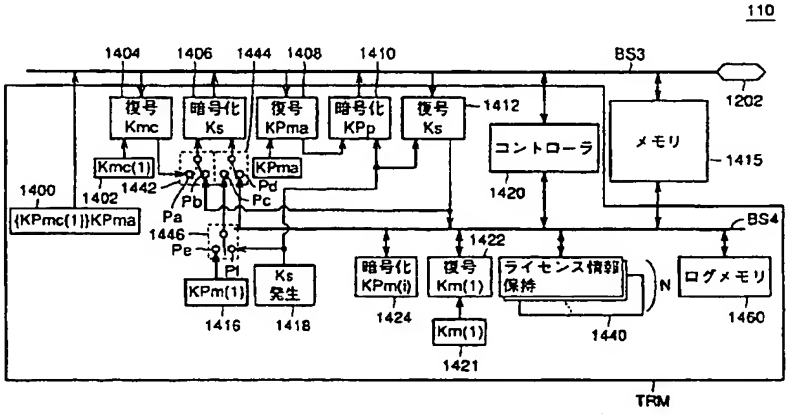
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 堀 吉宏 (HORI, Yoshihiro) [JP/JP]. 日置敏昭 (HIOKI, Toshiaki) [JP/JP]. 金森美和 (KANAMORI, Miwa) [JP/JP]. 吉川隆敏 (YOSHIKAWA, Takatoshi) [JP/JP]. 武村浩司 (TAKEMURA, Hiroshi) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP). 高橋政孝 (TAKAHASHI, Masataka) [JP/JP]; 〒929-1125 石川県河北郡宇ノ気町字宇野気ヌ98番地の2 株式会社 ピーエフユー内 Ishikawa (JP). 長谷部高行 (HASEBE, Takayuki) [JP/JP]. 古田茂樹 (FURUTA,

[続葉有]

(54) Title: MEMORY CARD AND DATA DISTRIBUTION SYSTEM USING IT

(54) 発明の名称: メモリカードおよびそれを用いたデータ配信システム



1404...DECRYPTION Kmc
1406...ENCRYPTION Ks
1408...DECRYPTION KPma
1410...ENCRYPTION KPp
1412...DECRYPTION Ks
1420...CONTROLLER
1415...MEMORY
1418...Ks GENERATION
1424...ENCRYPTION KPm(i)
1422...DECRYPTION Km(1)
1440...HOLDING OF LICENSE INFORMATION
1460...LOG MEMORY

(57) Abstract: A memory card (110) performs authentication with a server based on data held in an authentication data holding section (1400). The memory card (110) extracts a first cession key (Ks1) and a transaction ID from the server by decrypting data placed on a data bus (BS3). Furthermore, the memory card (110) generates a second cession key (Ks2) by means of a cession key generating section (1418), encrypts the second cession key (Ks2) and a key (KPm(1)) unique to the memory card (110) with the first cession key (Ks1) and transmits them to the server as keys for encrypting the content key when the content key is decrypted. The transaction ID and the second cession key (Ks2) held in a log memory (1460) are used in redistribution.

[続葉有]

WO 01/41356 A1

Shigeki) [JP/JP]. 畠山卓久 (HATAKEYAMA, Takahisa) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 利根川忠明 (TONEGAWA, Tadaaki) [JP/JP]; 〒187-8588 東京都小平市上水本町五丁目20番1号 株式会社 日立製作所 半導体グループ内 Tokyo (JP). 穴澤健明 (ANAZAWA, Takeaki) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内 Tokyo (JP).

(74) 代理人: 深見久郎, 外 (FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

(57) 要約:

メモリカード（１１０）は、認証データ保持部（１４００）に保持されるデータに基づいて、サーバとの間で認証処理を行なう。メモリカード（１１０）は、データバス（ＢＳ３）に与えられるデータから、復号処理をすることによりサーバからの第１のセッションキー（Ｋｓ１）およびトランザクションＩＤを抽出する。さらに、メモリカード（１１０）は、セッションキー発生部（１４１８）により第２のセッションキー（Ｋｓ２）を生成し、コンテンツキーの復号を受ける際にコンテンツキーを暗号化するための鍵として、第２のセッションキー（Ｋｓ２）およびメモリカード（１１０）に固有な鍵（ＫＰｍ（１））を第１のセッションキー（Ｋｓ１）で暗号化してサーバに送信する。ログメモリ（１４６０）に保持されるトランザクションＩＤおよび第２のセッションキー（Ｋｓ２）が、再配信処理で使用される。

明細書

メモリカードおよびそれを用いたデータ配信システム

技術分野

本発明は、携帯電話等の端末に対して情報を配送するための情報配信システムにおいて、コピーされた情報に対する著作権保護を可能とするメモリカードおよびそれを用いた配信システムに関するものである。

背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このような情報通信においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

つまり、このような情報通信網上において音楽情報や画像データ等の著作者の権利の存在するコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ところで、上述したようなデジタル情報通信網を介した音楽データなどのコンテンツデータの配信が行なわれた場合、各ユーザは、このようにして配信されたデータを何らかの記録装置に記録した上で、再生装置で再生することになる。

このような記録装置としては、たとえば、メモリカードのように電気的にデータの書込および消去が可能な媒体が用いられることになる。

さらに、配信された音楽データを再生する装置としては、このようなデータの配信を受けるのに用いた携帯電話機自身を用いる場合や、あるいは、記録装置がメモリカードなどのように配信を受ける装置から着脱可能な場合は、専用の再生装置を用いることも可能である。

いずれの場合にしても、デジタル情報通信網、特に無線による通信網を介して音楽データなどのコンテンツデータの配信をうける場合に、音楽データ等の全ての配信が完了する前に、通信回線の状態等によっては、通信が途絶してしまう場合があり得る。たとえば、コンテンツデータを暗号化した暗号化コンテンツデータと復号して再生に必要な再生情報として配信する場合、暗号化コンテンツデータの配信時における通信の途絶に際しては、再接続を行った後、継続してデータの受信を行えばよいが、再生情報の配信に際しては、ユーザに対する課金処理も同時に行われるため、このような通信途絶に対して、ユーザは再接続後に、再生情報の再送信を要求してくることになる。しかしながら、要求に対してむやみに再生情報の再送信を行うことは、著作権者の権利保護の観点から許されるべきでない。逆に、再送信は行わないものとすると、課金処理は行われたにも関わらず、ユーザが再生情報を取得できないというような問題が生じ得る。

発明の開示

この発明の他の目的は、、再生情報の配信が完了する前に、通信が途絶してしまった場合でも、著作権者の権利を保護した上で通信の再開により、再生情報の配信を完了させることが可能なデータ配信システムおよびそれに用いられるメモリカードを提供することである。

係る目的を達成するために本願発明に係るメモリカードは、暗号化コンテンツデータの再生に関連し、暗号化コンテンツデータを復号して平文にするためのコンテンツキーを含む再生情報を通信経路を介して受けて記録するためのメモリカードであって、データ通信部と、第１の記憶部と、情報抽出部と、第２の記憶部と、制御部とを備える。

データ通信部は、暗号化されて送られる再生情報の受信のために、再生情報の送信元との間での通信経路を確立する。第１の記憶部は、データ通信部から与えられる再生情報に関連するデータを保持する。情報抽出部は、データ通信部からの再生情報に関連するデータを第１の記憶部へ格納する処理を行い、かつ第１の記憶部に格納されたデータに基づいて、再生情報を抽出する。第２の記憶部は、再生情報の送信処理における処理状態を示す受信ログを記録する。制御部は、メモリカードの動作を制御する。制御部は、要求に応じて受信ログの送信元への送信を制御する。

好ましくは、データ通信部は、第１の鍵保持部と、第１の復号処理部と、第２の鍵保持部と、鍵生成部と、第１の暗号化処理部と、第２の復号処理部とを含む。第１の鍵保持部は、メモリカードに対応して予め定められた第１の公開暗号鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する。第１の復号処理部は、再生情報の通信ごとに更新されて送信され、第１の公開暗号鍵によって暗号化された第１の共通鍵を受けて、復号処理する。第２の鍵保持部は、メモリカードごとに異なる第２の公開暗号鍵を保持する。鍵生成部は、再生情報の通信ごとに更新して第２の共通鍵を生成する。第１の暗号化処理部は、第２の公開暗号鍵および第２の共通鍵を、第１の共通鍵に基づいて暗号化し、出力する。第２の復号処理部は、第２の公開暗号鍵で暗号化され、さらに第２の共通鍵で暗号化された再生情報を受け、第２の共通鍵に基づいて復号化する。第１の記憶部は、第２の復号処理部の出力に基づいたデータを保持する。情報抽出部は、第３の鍵保持部と、第３の復号処理部とを含む。第３の鍵保持部は、第２の公開暗号鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する。第３の復号処理部は、再生情報に関連するデータの第１の記憶部への格納処理から再生情報を抽出する処理までの過程において、第２の秘密復号鍵についての復号処理を行なう。

この発明のさらに他の局面に従うと、データ配信システムであって、コンテンツデータ供給装置と、複数の端末とを備える。

コンテンツデータ供給装置は、暗号化コンテンツデータと、暗号化コンテンツデータの再生に関連し、かつ暗号化コンテンツデータを復号して平文にするため

の復号鍵であるコンテンツキーを含む再生情報とを供給する。コンテンツデータ供給装置は、配信情報保持部と、第１のインタフェース部と、第１のセッションキー発生部と、セッションキー暗号化部と、セッションキー復号部と、第１のライセンスデータ暗号処理部と、第２のライセンスデータ暗号処理部と、配信ログ情報保持部とを含む。配信情報保持部は、コンテンツデータおよび再生情報を保持する。第１のインタフェース部は、外部との間でデータを授受する。第１のセッションキー発生部は、端末に対する再生情報の配信ごとに更新される第１の共通鍵を生成する。セッションキー暗号化部は、ユーザの端末に対応して予め定められた第１の公開暗号鍵により第１の共通鍵を暗号化して第１のインタフェース部に与える。セッションキー復号部は、第１の共通鍵により暗号化されて返信される第２の公開暗号鍵と第２の共通鍵とを復号する。第１のライセンスデータ暗号処理部は、暗号化コンテンツデータを再生するための再生情報を、セッションキー復号部により復号された第２の公開暗号鍵によって暗号化する。第２のライセンスデータ暗号処理部は、第１のライセンスデータ暗号処理部の出力を第２の共通鍵でさらに暗号化して第１のインタフェース部に与え配信する。配信ログ情報保持部は、配信処理中の処理状態を示す配信ログを記録する。複数の端末は、コンテンツデータ供給装置から、通信経路を介して配信を受け、複数のユーザにそれぞれ対応する。各端末は、第２のインタフェース部と、受信制御部と、データ格納部とを含む。第２のインタフェース部は、外部との間でデータ授受をする。受信制御部は、外部との間のデータ授受を制御する。データ格納部は、暗号化コンテンツデータと再生情報とを受けて格納する。データ格納部は、第１の鍵保持部と、第１の復号処理部と、第２の鍵保持部と、鍵生成部と、第１の暗号化処理部と、第２の復号処理部と、第１の記憶部と、第３の鍵保持部と、第３の復号処理部と、第２の記憶部とを有する。第１の鍵保持部は、データ格納部に対応して予め定められた第１の公開暗号鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する。第１の復号処理部は、再生情報の通信ごとに更新されて配信され、第１の公開暗号鍵によって暗号化された第１の共通鍵を受けて、復号処理する。第２の鍵保持部は、データ格納部ごとに異なる第２の公開暗号鍵を保持する。鍵生成部は、再生情報の通信ごとに更新して第２の共通鍵を生

成する。第１の暗号化処理部は、第２の公開暗号鍵および第２の共通鍵を、第１の共通鍵に基づいて暗号化し、出力する。第２の復号処理部は、第２の公開暗号鍵で暗号化され、さらに第２の共通鍵で暗号化された再生情報を受け、第２の共通鍵に基づいて復号化する。第１の記憶部は、第２の復号処理部の出力に基づいたデータを保持する。第３の鍵保持部は、第２の公開暗号鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する。第３の復号処理部は、再生情報に関連するデータの第１の記憶部への格納処理から再生情報を抽出する処理までの過程において、第２の秘密復号鍵についての復号処理を行なう。第２の記憶部は、暗号化コンテンツデータおよび再生情報の配信処理における処理状態を示す受信ログを記録する。受信制御部は、配信処理中に通信経路が切断された場合に、受信ログに基づいて再配信処理を制御する。

したがって、本発明に係るデータ再生装置を用いた配信システムおよびそれに用いるメモリカードでは、サーバおよびメモリカードがいずれも配信の履歴や配信の状態を保持しているので、通信が配信途中で途絶した場合でも、通信の再開により情報の再送信を可能とし、配信処理の信頼性を向上させることが可能となる。

図面の簡単な説明

図１は、本発明のデータ配信システムの全体構成を概略的に説明するための概念図である。

図２は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

図３は、ライセンスサーバ１０の構成を示す概略ブロック図である。

図４は、携帯電話機１００の構成を示す概略ブロック図である。

図５は、メモリカード１１０の構成示す概略ブロック図である。

図６は、実施例１に従うデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

図７は、実施例１に従うデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

図８は、実施例１に従うデータ配信システムにおける配信動作を説明するための第３のフローチャートである。

図９は、再接続処理を説明するためのフローチャートである。

図１０は、実施例１に従うデータ配信システムにおける、第２の再接続動作を説明するための第１のフローチャートである。

図１１は、実施例１に従うデータ配信システムにおける、第２の再接続動作を説明するための第２のフローチャートである。

図１２は、実施例１に従うデータ配信システムにおける、第２の再接続動作を説明するための第３のフローチャートである。

図１３は、実施例１に従うデータ配信システムにおける第３の再接続動作を説明するためのフローチャートである。

図１４は、再接続処理を説明するためのフローチャートである。

図１５は、実施例２に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第１のフローチャートである。

図１６は、実施例２に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第２のフローチャートである。

図１７は、実施例２に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第３のフローチャートである。

図１８は、実施例２に従うデータ配信システムにおける、第２の再接続動作を説明するための第１のフローチャートである。

図１９は、実施例２に従うデータ配信システムにおける、第２の再接続動作を説明するための第２のフローチャートである。

図２０は、実施例２に従うデータ配信システムにおける、第２の再接続動作を説明するための第３のフローチャートである。

図２１は、実施例３に従うデータ配信システムにおける、第２の再接続動作を説明するための第１のフローチャートである。

図２２は、実施例３に従うデータ配信システムにおける、第２の再接続動作を説明するための第２のフローチャートである。

図２３は、実施例３に従うデータ配信システムにおける、第２の再接続動作を

説明するための第３のフローチャートである。

図２４は、実施例３に従うデータ配信システムにおける、第２の再接続動作を説明するための第４のフローチャートである。

発明を実施するための最良の形態

以下、本発明の実施例を図面とともに説明する。

［実施例１］

図１は、本発明のデータ配信システムの全体構成を概略的に説明するための概念図である。

なお、以下では携帯電話網を介して音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他のコンテンツデータ、朗読データ、画像データ、映像データ、教材データ等を、他の情報通信網を介して配信する場合にも適用することが可能なものである。

図１を参照して、著作権の存在する音楽データを管理するライセンスサーバ１０は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、情報を配信するための配信キャリア２０である携帯電話会社に、このような暗号化データを与える。一方、認証サーバ１２は、コンテンツデータの配信を求めてアクセスしてきたユーザが正規の機器を用いてアクセスしたか否かの認証を行なう。

携帯電話会社２０は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）をライセンスサーバ１０に中継する。ライセンスサーバ１０は、配信リクエストがあると、認証サーバ１２によりユーザが正規の機器からアクセスしていることを確認し、要求された音楽データをさらに暗号化した上で携帯電話会社２０の携帯電話網を介して、各ユーザの携帯電話機に対してコンテンツデータを配信する。

図１においては、たとえば携帯電話ユーザ１の携帯電話機１００には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取って、上記送

信にあたって行なわれた暗号化については復号した上で、携帯電話機１００中の音楽再生回路（図示せず）に与える。

さらに、たとえばユーザ１は、携帯電話機１００に接続したヘッドホン１３０等を介してこのような音楽データを「再生」して、聴取することが可能である。

以下では、このようなライセンスサーバ１０と認証サーバ１２と配信キャリア（携帯電話会社）２０と併せて、配信サーバ３０と総称することにする。

また、このような配信サーバ３０から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

このような構成とすることで、まず、メモリカード１１０を所持していないユーザは、配信サーバ３０からの配信データを受取って再生することができない構成となる。

しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

しかも、このようなコンテンツデータの配信は、携帯電話網というクローズなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

このとき、たとえばメモリカード１１２を有するユーザ２が自己の携帯電話機１０２により、配信サーバ３０から直接コンテンツデータの配信を受けることは可能である。しかしながら、相当量のデータ量を有するコンテンツデータ等をユーザ２が直接配信サーバ３０から受信することとすると、この受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けているユーザ１から、そのコンテンツデータをコピーできることを可能としておけば、ユーザにとっての利便性が向上する。

しかしながら、著作権者の権利保護の観点からは、自由なコンテンツデータのコピーを放任することはシステム構成上許されない。

図１に示すように、ユーザ１が受信したコンテンツデータを、コンテンツデー

タそのものおよび当該コンテンツデータを再生可能とするために必要な再生情報とともに、ユーザ２に対してコピーさせる場合を音楽データの「移動」と呼ぶ。この場合に、携帯電話機１００および１０２を介して、メモリカード１１０と１１２との間で暗号化されたコンテンツデータおよび再生のために必要な再生情報が移動される。ここで、「再生情報」は、後に説明するように、所定の暗号化方式に従って暗号化されたコンテンツデータを復号可能なライセンスキーと、アクセス再生に関する制限情報やコンテンツＩＤ等のライセンス情報とを有する。

これに対して、再生情報の移動を伴わない、すなわち、コンテンツデータのみをコピーすることを「複製」と呼ぶ。複製では再生情報の移動を伴わないため、複製を受けたユーザは、配信サーバ３０に対して再生情報のみの配信を要求すれば、再生できる状態となる。この場合、コンテンツデータの配信における相当量のデータの配信を省くことができる。

このような構成とすることによって、一旦配信サーバより配信を受けたコンテンツデータについて受信者側での柔軟な利用が可能となる。

また、携帯電話機１００および１０２がＰＨＳ（Personal Handy Phone）である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ１とユーザ２との間における情報の移動を行なうことが可能である。

図１に示したような構成においては、暗号化して配信されるコンテンツデータをユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号鍵を配信するための方式であり、さらに第２には、配信データを暗号化する方式そのものであり、さらに、第３には、このように配信されたデータの無断コピーを防止するためのデータ保護を実現する構成である。

本発明の実施例においては、特に、配信中の状態、履歴を情報の送信側および受信側の双方で記録保持し、通信が配信途中で途絶した場合でも、通信の再開により情報の再送信を可能とし、配信処理の信頼性を向上させることが可能な配信システムについて説明する。

［システムの鍵およびデータの構成］

図２は、図１に示したデータ配信システムにおいて、使用される通信のための

データ、情報等の特性を説明する図である。

まず、配信サーバ３０より配信されるデータ Data は、音楽データ等のコンテンツデータである。コンテンツデータ Data は、後に説明するように、少なくともライセンスキーKc によって復号可能な暗号化が施された暗号化コンテンツデータ {Data} Kc という形式で、配信サーバ３０よりユーザに配布される。

なお、以下においては、{Y} X という表記は、データ Y を、鍵データ X により復号可能な暗号に変換した情報であることを示すものとする。

さらに、配信サーバからは、コンテンツデータとともに、コンテンツデータに関する、あるいはサーバアクセス関連等の平文情報としての付加情報 Data-inf が配布される。すなわち、付加情報 Data-inf には、コンテンツデータの曲目やアーティスト名などコンテンツデータを特定するための情報や、配信サーバ３０が、いずれのサーバであるかを特定するための情報等が含まれる。

次に、コンテンツデータの暗号化や復号・再生処理や、再生回路である携帯電話機や記録媒体であるメモリカードの認証に関わる鍵として、以下のものがある。

すなわち、上述したとおり、暗号化コンテンツデータを復号するためのライセンスキーＫｃと、コンテンツ再生回路（携帯電話機１００）に固有な公開暗号鍵 KPp（n）と、メモリカードに固有な公開暗号鍵 KPmc（m）とがそれぞれ設けられる。

公開暗号鍵 KPp（n）および KPmc（m）により暗号化されたデータは、コンテンツ再生回路（携帯電話機１００）の固有の秘密復号鍵 Kp（n）およびメモリカード固有の秘密復号鍵 Kmc（m）によってそれぞれ復号可能である。これら固有の秘密復号鍵は、携帯電話機の種類ごとおよびメモリカードの種類ごとに異なる内容を有する。ここで、携帯電話機やメモリカードの種類とは、それらを製造するメーカや製品の種類や、製造時期（製造ロット）の違い等に基づき規定される。この公開暗号鍵および秘密復号鍵の付与される単位をクラスと呼ぶものとする。自然数 m、n は、それぞれ各メモリカードおよびコンテンツ再生回路（携帯電話機）のクラスを区別するための番号を表わす。

さらに、配信システム全体で共通に運用される鍵として、主としてライセンスキーKc や後に説明する再生回路に対する制限情報などの取得に利用される秘密

共通鍵 Kcom と、認証鍵 KPma とが存在する。秘密共通鍵 Kcom は、配信サーバと携帯電話機との双方で保持される。

なお、上述したメモリカードおよびコンテンツ再生回路ごとに設定される公開暗号鍵 KPmc (m) および KPp (n) は、認証鍵ＫＰｍａにて復号することで、その正当性が確認できる。すなわち認証処理の対象となる認証データ {KPmc (m) } KPma および {KPp (n) } KPma の形式で、出荷時にメモリカードおよび携帯電話機にそれぞれ記録される。

なお、秘密共通鍵 Kcom は共通鍵方式に限定されず、公開鍵方式における秘密復号鍵と公開暗号鍵ＫＰｃｏｍに置き換えて運用することも可能である。この場合、携帯電話機１００には秘密復号鍵 Kcom が、配信サーバ３０には、公開暗号鍵 Kpcom が暗号鍵として保持される。

さらに、システムを構成する機器、すなわち、コンテンツ再生回路である携帯電話機１００やメモリカード１１０の動作を制御するための情報として、利用者がライセンスキー等を購入する際に、携帯電話機１００から配信サーバ３０に対してその購入条件を指定するために送信される購入条件ＡＣと、購入条件ＡＣに応じて、配信サーバ３０からメモリカード１１０に対して配信され、再生のためにライセンスキーＫｃにアクセスする回数（再生許諾回数）やライセンスキーＫｃの複製・移動回数やコピー、移動に対する制限を示すアクセス制限情報ＡＣ１と、配信サーバ３０から携帯電話機１００に対して配信され、再生回路の再生条件の制限を示す再生回路制限情報ＡＣ２とが存在する。再生回路の再生条件とは、たとえば、新曲のプロモーションとして廉価にまたは無償でサンプルを配信する場合などに、各コンテンツデータの冒頭の所定時間のみの再生の許可や再生期限等の条件を意味する。

また、メモリカード１００内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに個別に設定されるメモリカードごとに固有の公開暗号鍵 KPm (i) (i・自然数) と、公開暗号鍵 KPm (i) で暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵 Km (i) とが存在する。ここで、自然数ｉは、各メモリカードを区別するための番号を表わす。

さらに、図１に示したデータ配信システムにおいて、データの通信時に使用さ

れる鍵等として以下のものがある。

すなわち、メモリカード外とメモリカード間でのデータ授受における秘密保持のための鍵として、コンテンツデータの配信、再生および移動が行なわれるごとにサーバ３０、携帯電話機１００または１０２、メモリカード１１０または１１２において生成される共通鍵Ks１～Ks４が用いられる。

ここで、共通鍵 Ks１～Ks４は、サーバ、携帯電話もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵 Ks１～Ks４を「セッションキー」とも呼ぶこととする。

これらのセッションキーKs１～Ks４は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。

具体的には、セッションキーKs１は、配信サーバ３０によって配信セッションごとに発生される。セッションキーKs２は、メモリカードによって配信セッションおよび移動（受信側）セッションごとに発生し、セッションキーKs３は、同様にメモリカードにおいて再生セッションおよび移動（送信側）セッションごとに発生する。セッションキーKs４は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンスキー等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

さらに、配信サーバとの間で授受されるデータとしては、コンテンツデータをシステムが識別するためのコンテンツＩＤや、再生情報の発行がいつ、誰に対して行なわれたかを特定し、配信セッションごとに生成され、各配信セッションを特定するためのコードであるトランザクションＩＤなどがある。尚、ライセンスＩＤとトランザクションＩＤは兼用してもかまわない。

ライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１を総じてライセンス情報と称し、このライセンス情報とライセンスキーＫｃおよび再生回路制限情報ＡＣ２を総じて再生情報と称する。

［ライセンスサーバ１０の構成］

図３は、図１に示したライセンスサーバ１０の構成を示す概略ブロック図である。

ライセンスサーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータや、コンテンツ ID 等の配信情報を保持するための情報データベース３０４と、各ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、ライセンスサーバのログ情報を保持するためのログ管理データベース３０６と、情報データベース３０４、課金データベース３０２およびログ管理データベース３０６からのデータをデータバス BS１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

ここで、ログ管理データベース３０６に保持されるライセンス情報の配信の履歴を示す「ライセンス配信ログ」としては、トランザクションＩＤ、コンテンツＩＤ、公開暗号鍵 KPmc(n)、KPp(n)、アクセス制限情報 AC1、再生回路制限情報 AC2、公開暗号鍵 KPm(i)、セッションキーKs2、課金状態フラグ等の情報がある。課金状態フラグは、配信中のコンテンツデータについての課金処理がすでに終了しているか否かをしめすフラグである。

データ処理部３１０は、データバス BS１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーKs１を発生するためのセッションキー発生部３１６と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ｛KPmc（n）｝KPma および｛KPp（n）｝KPma を通信装置３５０およびデータバス BS１を介して受けて、認証鍵 KPma に対する復号処理を行なう復号処理部３１２と、セッションキー発生部３１６より生成されたセッションキーKs１を復号処理部３１２によって得られた公開暗号鍵 KPmc（m）を用いて暗号化して、データバス BS１に出力するための暗号化処理部３１８と、各ユーザにおいてセッションキーKs１によって暗号化された上で送信されたデータをデータバス BS１をより受けて、復号処理を行なう復号処理部３２０とを含む。

データ処理部３１０は、さらに、秘密共通鍵Kcomを保持するKcom保持部３２２と、配信制御部３１５から与えられるライセンスキーKc および再生回路制限情報 AC２を秘密共通鍵 Kcom によって暗号化する暗号化処理部３２４と、暗号化処理部３２４から出力されたデータを復号処理部３２０によって得られたメモリカード固有の公開暗号鍵 KPm（i）によって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーKs２によってさらに暗号化してデータバス BS１に出力するための暗号化処理部３２８とを含む。

なお、秘密共通鍵 Kcom を非対称な公開鍵暗号系の鍵とする場合においては、鍵データを保持する保持部３２２は、共通鍵方式における秘密共通鍵 Kcom に代えて公開鍵方式における暗号鍵である公開暗号鍵KPcomを保持する。

［携帯電話機１００の構成］

図４は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

携帯電話機１００においては、クラスを表わす自然数ｎは、ｎ＝１とする。

携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのデータバス BS２と、データバス BS２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６とを含む。

携帯電話機１００は、さらに、外部からの指示を携帯電話機１００に与えるためのキーボード１１０８と、コントローラ１１０６等から出力される情報をユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データバス BS２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２と、外部との間でデータの授受を行なうためのコネクタ１１２０と、コネクタ１１２０からのデータをデータバス BS２に与え得る信号に変換し、または、データバス BS２からのデータをコネクタ１１２０に与え得る信号に変換するための外部インタフェース部１１２２とを含む。

携帯電話機１００は、さらに、配信サーバ３０からのコンテンツデータ（音楽データ）を記憶し、かつ復号処理するための着脱可能なメモリカード１１０と、メモリカード１１０とデータバス BS２との間のデータの授受を制御するためのメモリインタフェース１２００と、携帯電話機のクラスごとに設定される公開暗号鍵 KPp（1）を、認証鍵 KPma で復号することで認証可能な状態に暗号化したデータを保持する認証データ保持部１５００を含む。

携帯電話機１００は、さらに、携帯電話機（コンテンツ再生回路）のクラス固有の復号鍵である秘密復号鍵 Kp（n）（ｎ＝１）を保持する Kp 保持部１５０２と、データバス BS２から受けたデータを秘密復号鍵 Kp（1）によって復号し、メモリカードによって発生されたセッションキーKs３を得る復号処理部１５０４と、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいて、メモリカード１１０との間でデータバス BS２上においてやり取りされるデータを暗号化するためのセッションキーKs４を乱数等により発生するセッションキー発生部１５０８と、生成されたセッションキーKs４を復号処理部１５０４によって得られたセッションキーKs３によって暗号化しデータバス BS２に出力する暗号化処理部１５０６と、データバス BS２上のデータをセッションキーKs４によって復号して、データ｛Kc//AC２｝Kcom を出力する復号処理部１５１０とをさらに含む。

携帯電話機１００は、さらに、秘密共通鍵 Kcom を保持する Kcom 保持部１５１２と、復号処理部１５１０が出力するデータ｛Kc//AC２｝Kcom を秘密共通鍵 Kcom で復号し、ライセンスキーKc および再生回路制限情報 AC２を出力する復号処理部１５１４と、データバス BS２より暗号化された暗号化コンテンツデータ｛Data｝Kc を受けて、復号処理部１５１４より取得してライセンスキーKc によって復号しコンテンツデータＤａｔａを出力する復号処理部１５１６と、復号処理部１５１６の出力であるコンテンツデータＤａｔａを受けて音楽を再生するための音楽再生部１５１８と、音楽再生部１５１８と音声再生部１１１２の出力を受けて、動作モードに応じて選択的に出力するための切換部１５２５と、切換部１５２５の出力を受けて、ヘッドホン１３０と接続するための接続端子１５３０とを含む。

ここで、復号処理部１５１４から出力される再生回路制限情報 AC２は、データバスＢＳ２を介して、コントローラ１１０６に与えられる。

なお、図４においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては一部割愛している。

［メモリカード１１０の構成］

図５は、図１に示したメモリカード１１０の構成を説明するための概略ブロック図である。

既に説明したように、公開暗号鍵 KPm（i）およびこれに対応する秘密復号鍵 Km（i）は、メモリカードごとに固有の値であるが、メモリカード１１０においては、この自然数 i＝１であるものとする。また、メモリカードのクラスに固有の公開暗号鍵および秘密復号鍵として、KPmc（m）および Kmc（m）が設けられるが、メモリカード１１０においては、自然数 m は、m＝１で表わされるものとする。

メモリカード１１０は、認証データ｛KPmc（１）｝KPma を保持する認証データ保持部１４００と、メモリカードのクラスごとに設定される固有の復号鍵である Kmc（１）を保持する Kmc 保持部１４０２と、メモリカードごとに固有に設定される公開暗号化鍵 ＫＰm（１）を保持する ＫＰm（１）保持部１４１６と、公開暗号化鍵 ＫＰm（１）によって復号できる非対称な秘密復号鍵 Km（１）を保持する Km（１）保持部１４２１とを含む。ここで、認証データ保持部１４００は、メモリカードのクラスごとに設定される公開暗号鍵 KPmc（1）を認証鍵 KPma で復号することでその正当性を認証できる暗号化を行って保持する。

メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１２０２を介して授受するデータバス BS３と、データバス BS３にメモリインタフェース１２００から与えられるデータから、メモリカードのクラスごとに固有の秘密復号鍵 Kmc（１）を Kmc（１）保持部１４０２から受けて配信サーバが配信セッションにおいて生成したセッションキーKs３を接点 Pa に出力する復号処理部１４０４と、KPma 保持部１４４３から認証鍵 KPma を受けて、データバス BS３に与えられるデータから認証鍵 KPma による復号処理を実行して復号結

果を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵データによって、切換スイッチ１４４４によって選択的に与えられるデータを暗号化してデータバス BS３に出力する暗号化処理部１４０６とを含む。

メモリカード１１０は、さらに、配信、再生および移動の各セッションにおいてセッションキーを発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーを復号処理部１４０８によって得られる公開暗号鍵 KPp（n）によって暗号化してデータバス BS３に出力する暗号化処理部１４１０と、BS３より暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーKs３によって復号し、復号結果をデータバス BS４に送出する復号処理部１４１２とを含む。

メモリカード１１０は、さらに、配信や移動セッション等においてデータバス BS４上のデータをメモリカード固有の公開暗号鍵 KPm(ｉ)（ｉは、１あるいは他のメモリカードの番号ｊも可能）で暗号化する暗号化処理部１４２４と、データバス BS４上のデータを公開暗号鍵 KPm（１）と対をなすメモリカード１１０固有の秘密復号鍵 Km（１）によって復号するための復号処理部１４２２と、公開暗号鍵 KPm（１）で暗号化されている再生情報（ライセンスキーKc、コンテンツ ID、トランザクション ID、アクセス制限情報 AC１、再生回路制限情報 AC２）の一部をデータバス BS４より受けて格納するとともに、暗号化コンテンツデータ {Data} Kc をデータバス BS３より受けて格納するためのメモリ１４１５とを含む。

携帯電話機１１０は、さらに、復号処理部１４２２によって得られるライセンス情報（トランザクション ID、コンテンツ ID およびアクセス制限情報 AC１）を保持するためのライセンス情報保持部１４４０と、メモリカードにおける再生情報の送受信に関するログを保持するためのログメモリ１４６０と、データバス BS３を介して外部との間でデータ授受を行ない、データバス BS４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを含む。

ログメモリ１４６０に保持される再生情報の受信状態を示す「受信ログ」とし

ては、トランザクションＩＤやセッションキーKs2 等がある。実施例１では、これらの受信ログ情報は、ライセンスの受信が行なわれる際に生成されるデータであり、再生情報のメモリカード１１０への受信および保存が完了した時点で、消去される。

なお、図５において、実線で囲んだ領域 TRM は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュール TRM に組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュール（Tamper Resistance Module）である。

もちろん、メモリ１４１５も含めて、モジュール TRM 内に組込まれる構成としてもよい。しかしながら、図５に示したような構成とすることで、メモリ１４１５中に保持されているデータは、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１５中のデータのみでは、コンテンツデータから音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ１４１５を設ける必要がないので、製造コストが低減されるという利点がある。

［配信動作］

次に、本発明の実施例に従うデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

図６、図７および図８は、実施例１に従うデータ配信システムにおけるコンテンツデータの購入時に発生する配信動作（以下、配信セッションともいう）を説明するための第１、第２および第３のフローチャートである。

図６～図８においては、ユーザ１が、メモリカード１１０を用いることで、携帯電話機１００を介して配信サーバ３０から音楽データの配信を受ける場合の動作を説明している。

まず、ユーザ１が、携帯電話機１００のキーボード１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

メモリカード１１０においては、この配信リクエストに応じて、認証データ保

持部１４００より認証データ｛KPmc（１）｝KPma が出力される（ステップＳ１０２）。

携帯電話機１００は、メモリカード１１０から受理した認証のための認証データ｛KPmc（１）｝KPma に加えて、携帯電話機１００自身の認証のための認証データ｛KPp（１）｝KPma と、コンテンツ ID、ライセンス購入条件 AC とを配信サーバ３０に対して送信する（ステップＳ１０４）。

配信サーバ３０では、携帯電話機１００からコンテンツ ID、認証データ｛KPmc（１）｝KPma、｛KPp（１）｝KPma、ライセンス購入条件 AC を受信し（ステップＳ１０６）、復号処理部３１２において認証鍵 KPma で復号処理を実行して、メモリカード１１０の公開暗号鍵である KPmc（１）と、携帯電話機１００の公開暗号鍵である KPp（１）とを受理する（ステップＳ１０８）。

配信制御部３１５は、受理した公開暗号鍵 KPmc（１）および KPp（１）に基づいて、認証サーバ１２に対して照会を行ない（ステップＳ１１０）、これらの公開暗号鍵が有効である場合には次の処理（ステップＳ１１２）に移行し、これらの公開暗号鍵が無効である場合には、処理を終了する（ステップＳ１７０）。

ここで、認証鍵 KPma による復号処理において、公開暗号鍵 KPp(1)あるいは KPmc(1)の正当性の認証が行なわれるにあたり、認証サーバ１２に照会を行うとしたが、公開暗号鍵 KPp(1)あるいは KPmc(1)は、それぞれが認証鍵 KPma によって復号することでその正当性が判断可能な暗号化が施されているため、ライセンスサーバ１０の配信制御部３１５が認証鍵ＫＰｍａによる復号結果から独自に認証を行う構成としてもよい。

照会の結果、正規のメモリカードへの配信であることが認識されると、配信制御部３１５は、次に、配信セッションを特定するためのトランザクションＩＤを生成する（ステップＳ１１２）。

照会の結果、正規のメモリカードへの配信であることが確認されると、さらに、配信制御部３１５は、トランザクション ID、コンテンツ ID、公開暗号鍵 KPmc(1),KPp(1)を、未課金であるとの情報（課金状態フラグ）とともに、ライセンス配信ログとして管理データベース３０６に記録する（ステップＳ１１３）。

続いて、配信サーバ３０において、セッションキー発生部３１６は、配信のた

めのセッションキーKs１を生成する。セッションキーKs１は、復号処理部３１２によって得られたメモリカード１１０に対応する公開暗号鍵KPmc（１）により、暗号化処理部３１８によって暗号化される（ステップＳ１１４）。

トランザクションＩＤと暗号化されたセッションキー｛Ks１｝Kmc（１）とは、データバス BS１および通信装置３５０を介して外部に出力される（ステップＳ１１６）。

携帯電話機１００が、トランザクションＩＤおよび暗号化されたセッションキー｛Ks１｝Kmc（１）を受信すると（ステップＳ１１８）、メモリカード１１０においては、メモリインタフェース１２００を介して、受信データをデータバスBS３に与える。復号処理部１４０４が、保持部１４０２に保持されるメモリカード１１０固有の秘密復号鍵 Kmc（１）により｛Ks１｝Kmc（１）を復号処理することにより、セッションキーKs１を復号し抽出し、結果、トランザクションＩＤとセッションキーＫｓ１を受理する（ステップＳ１２０）。

ここまでのステップＳ１２０までの処理を、「トランザクションＩＤ取得ステップ」と呼ぶことにする。

図７を参照して、コントローラ１４２０は、配信サーバ３０で生成されたセッションキーKs１の受理を確認すると、セッションキー発生部１４１８に対して、メモリカードにおいて配信動作時に生成されるセッションキーKs２の生成を指示する。さらに、コントローラ１４２０は、セッションキーKs２を、受け取ったトランザクション ID とともに受信
ログとして、ログメモリ１４６０に記録する（ステップＳ１２１）。

暗号化処理部１４０６は、切換スイッチ１４４２の接点 Pa を介して復号処理部１４０４より与えられるセッションキーKs１によって、切換スイッチ１４４４および１４４６の接点を順次切換えることによって与えられるセッションキーKs２および公開暗号鍵 KPm（１）を暗号化して、｛Ks２//KPm（１）｝Ks１をデータバスBS３に出力する（ステップＳ１２２）。

データバス BS３に出力された暗号データ｛Ks２//KPm（１）｝Ks１は、データバス BS３から端子１２０２およびメモリインタフェース１２００を介して携帯電話機１００に送信され、携帯電話機１００から配信サーバ３０に送信される

（ステップＳ１２４）。

配信サーバ３０は、暗号化データ｛Ks２//KPm（１）｝Ks１を受信して、復号処理部３２０においてセッションキーKs１による復号処理を実行し、メモリカードで生成されたセッションキーKS２およびメモリカード１１０固有の公開暗号鍵KPm（１）を受理する（ステップＳ１２６）。

さらに、配信制御部３１５は、ステップＳ１０６で取得したコンテンツ ID およびライセンス購入条件データ AC に従って、アクセス制限情報 AC１および再生回路制限情報 AC２を生成する（ステップＳ１３０）。さらに、暗号化コンテンツデータを復号するためのライセンスキーKc を情報データベース３０４より取得する（ステップＳ１３２）。

配信制御部３１５は、取得したライセンスキーKc および再生回路制限情報 AC２を暗号化処理部３２４に与える。暗号化処理部３２４は、Kcom 保持部３２２より得られる、秘密共通鍵 Kcom によって、ライセンスキーKc および再生回路制限情報 AC２を暗号化する（ステップＳ１３４）。

暗号化処理部３２４が出力する暗号化データ｛Kc//AC２｝Kcom と、配信制御部３１５が出力するトランザクション ID、コンテンツ ID およびアクセス制限情報 AC１とは、暗号化処理部３２６によって、復号処理部３２０によって得られたメモリカード１１０固有の公開暗号鍵 KPm（１）によって暗号化される（ステップＳ１３６）。

暗号化処理部３２８は、暗号化処理部３２６の出力を受けて、メモリカード１１０において生成されたセッションキーKs２によって暗号化する（ステップＳ１３７）。

配信制御部３１５は、ログデータ管理データベース３０６に、アクセス制限情報 AC1、再生回路制限情報 AC2、公開暗号鍵 KPm(1)、セッションキーKs2 を、課金済の情報（課金状態フラグ）とともに記録する（ステップＳ１３８）。

暗号化処理部３２８より出力された暗号化データ｛｛｛Kc//AC２｝Kcom//トランザクションＩＤ//コンテンツＩＤ//AC1｝Km(1)｝Ks2 は、データバス BS１および通信装置３５０を介して携帯電話機１００に送信される（ステップＳ１３９）。

このように、送信サーバおよびメモリカードでそれぞれ生成されるセッション

キーをやりとりし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。さらに、配信サーバ３０では、課金状態、配信の履歴に関する情報が記録保持されることになる。

携帯電話機１００は、送信された暗号化データ｛｛｛Kc//AC２｝Kcom//トランザクションＩＤ//コンテンツＩＤ//AC1｝Km(1)｝Ks2 を受信し（ステップＳ１４０）、メモリカード１１０においては、メモリインタフェース１２００を介して、データバス BS３に与えられた受信データを復号化処理部１４１２によって復号する。すなわち、復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーKs２を用いてデータバス BS３の受信データを復号しデータバス BS４に出力する（ステップＳ１４４）。

図８を参照して、ステップＳ１４４の段階で、データバス BS４には、Km（１）保持部１４２１に保持される秘密復号鍵 Km（１）で復号可能なデータ｛｛Kc//AC２｝Kcom//ライセンスＩＤ//コンテンツＩＤ//AC1｝Km(1)が出力されている。このデータ｛｛Kc//AC２｝Kcom//トランザクションＩＤ//コンテンツＩＤ//AC1｝Km(1)が、まず秘密復号鍵 Km(1)により復号され、再生情報であるデータ｛Kc//AC２｝Kcom、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報 AC1 が受理される（ステップＳ１４６）。

トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報 AC1 が、ライセンス情報保持部１４４０に記録される。データ｛Kc//AC２｝Kcom は、再び、公開暗号鍵 KPm(1)により暗号化され、データ｛｛Kc//AC２｝Kcom｝Km(1)としてメモリ１４１５に格納される（ステップ
）。

さらに、ログメモリ１４６０中の受信ログは消去される（ステップＳ１５０）。

ステップＳ１２１からステップＳ１５０までの処理を「再生情報取得ステップ」と呼ぶことにする。この「再生情報取得ステップ」では、課金対象の処理を行なう。

ステップＳ１５０までの処理が正常に終了した段階で、携帯電話機１００から

配信サーバ３０にコンテンツデータの配信要求がなされる（ステップＳ１５２）。

配信サーバ３０は、コンテンツデータの配信要求を受けて、情報データベース３０４より、暗号化コンテンツデータ {Data} Kc および付加情報 DATA-inf を取得して、これらのデータをデータバス BS1 および通信装置３５０を介して出力する（ステップＳ１５４）。

携帯電話機１００は、{Data} Kc／／Data-inf を受信して、暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf を受理する（ステップＳ１５６）。暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf はメモリインタフェース１２００および端子1,２０２を介してメモリカード１１０のデータバス BS3 に伝達される。メモリカード１１０においては、受信した暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf がそのままメモリ１４１５に格納される（ステップＳ１５８）。

ステップＳ１５２からステップＳ１５８までの処理を「コンテンツデータ取得ステップ」と呼ぶことにする。この「コンテンツデータ取得ステップ」では、課金対象外の処理を行なう。

さらに、メモリカード１１０から配信サーバ３０へは、配信受理の通知が送信され（ステップＳ１６０）、配信サーバ３０で配信受理を受信すると（ステップＳ１６２）、課金データベース３０２への課金データの格納等を伴って、配信終了の処理が実行され（ステップＳ１６４）、配信サーバの処理が終了する（ステップＳ１７０）。

［再接続動作］

つづいて、以上説明した配信動作のいずれか処理ステップの段階で、通信回線が途絶した場合に、再度、配信を受けるために再接続が行なわれる場合の処理を説明する。図９は、再接続処理を説明するためのフローチャートである。

まず、たとえば、ユーザ１が、携帯電話機１００のキーボード１１０８のキーボタンの操作等によって、再接続のリクエストがなされ、再接続処理が開始される（ステップＳ２００）。

つづいて、携帯電話機１００のコントローラ１１０６は、通信が切断したステップが、いずれの処理中であったかを判断し（ステップＳ２０２）、それがトラ

ンザクション ID 取得ステップであれば、課金の対象となっていないので図６～図８の基本配信処理（第１の再接続処理）を再度やり直し（ステップＳ２０４）、再接続処理が終了する（ステップＳ２０６）。

一方、コントローラ１１０６は、通信が切断したステップが、ライセンス取得ステップであれば（ステップＳ２０２）、後に説明する受信ログに基づく第２の再接続処理を行ない（ステップＳ２０６）、または、コンテンツデータ取得ステップであれば（ステップＳ２０２）、後に説明する通信の切断時における通信を継続して行うための第３の再接続処理を行ない（ステップＳ２０６）、再接続処理が終了する（ステップＳ２１０）。

［第２の再接続処理］

図１０、図１１および図１２は、実施例１に従うデータ配信システムにおける、上述した第２の再接続動作を説明するための第１、第２および第３のフローチャートである。ライセンスサーバ１０のライセンス配信ログとメモリカード１１０の受信ログを対比することで、通信切断時における再生情報の配信状態を確認し、著作権者の権利を保護しつつ、ユーザへの保証を実現するものである。

まず、図１０を参照して、ユーザ１が携帯電話機１００のキーボード１１０８のキーボタンの操作等によって、再接続リクエストがなされ、これに応じて第２の再接続処理が開始される（ステップＳ３００）。

メモリカード１１０においては、この再接続リクエストに応じて、ログメモリ１４６０に保持されたトランザクションＩＤが出力される（ステップＳ３０２）。

携帯電話機１００は、メモリカード１１０から受理したトランザクションＩＤを配信サーバ３０に対して送信する（ステップＳ３０４）。

配信サーバ３０では、トランザクションＩＤを受信し（ステップＳ３０６）、配信制御部３１５が、ログ管理データベース３０６中のライセンス配信ログを検索する（ステップＳ３０８）。

配信制御部３１５は、受信したトランザクションＩＤから再接続の要求をしてきた端末（携帯電話機１００およびメモリカード１１０）に対して課金処理がすでに行なわれている場合（ステップＳ３０８）、ライセンス配信ログから公開暗号鍵 KPmc（j）を取得する（ステップＳ３１０）。

セッションキー発生部３１６は、配信のためのセッションキーKs１を生成する。セッションキーKs１は、公開暗号鍵 KPmc（１）により、暗号化処理部３１８によって暗号化される（ステップＳ３１２）。

トランザクションＩＤと暗号化されたセッションキー｛Ks１｝Kmc（１）とは、データバス BS１および通信装置３５０を介して外部に出力される（ステップＳ３１４）。

携帯電話機１００が、トランザクションＩＤおよび暗号化されたセッションキー｛Ks１｝Kmc（１）を受信すると（ステップＳ３１６）、メモリカード１１０においては、メモリインタフェース１２００を介して、データバス BS３に与えられた受信データを、復号処理部１４０４が、保持部１４０２に保持されるメモリカード１１０固有の秘密復号鍵 Kmc（１）により復号処理することにより、セッションキーKs１を復号し抽出する（ステップＳ３１８）。

以後は、図７に示したステップＳ１２１以降の処理、すなわち、ライセンス取得ステップ以降の処理と同様の処理が行なわれる。

一方、ステップ３０８において、配信制御部３１５が、ログ管理データベース３０６中のライセンス配信ログを検索した結果、課金処理が終了していないと判断すると、ライセンス配信ログから公開暗号鍵 KPmc（１）を取得する（ステップＳ３３０）。

続いて、配信サーバ３０において、セッションキー発生部３１６は、配信のためのセッションキーKs１を生成する。セッションキーKs１は、公開暗号鍵 KPmc（１）により、暗号化処理部３１８によって暗号化される（ステップＳ３３２）。

トランザクションＩＤと暗号化されたセッションキー｛Ks１｝Kmc（１）とは、データバス BS１および通信装置３５０を介して外部に出力される（ステップＳ３３４）。

携帯電話機１００が、トランザクションＩＤおよび暗号化されたセッションキー｛Ks１｝Kmc（１）を受信すると（ステップＳ３３６）、メモリカード１１０においては、メモリインタフェース１２００を介して、データバス BS３に与えられた受信データを、復号処理部１４０４が、保持部１４０２に保持されるメモリカード１１０固有の秘密復号鍵 Kmc（１）により復号処理することにより、セ

ッションキーKs１を復号し抽出する（ステップＳ３３８）。

暗号化処理部１４０６は、受信ログをセッションキーＫｓ１で暗号化し、｛受信ログ｝Ksl を生成する（ステップＳ３４０）。

図１１を参照して、コントローラ１４２０は、セッションキー発生部１４１８に対して、メモリカードにおいて配信動作時に生成されるセッションキーKs２´の生成を指示する（ステップＳ３４２）。

暗号化処理部１４０６は、切換スイッチ１４４２の接点 Pa を介して復号処理部１４０４より与えられるセッションキーKs１によって、切換スイッチ１４４４および１４４６の接点を介して与えられるセッションキーKs２´を暗号化して、｛Ks２´｝Ks１を生成する。以上のようにして生成されたデータ｛受信ログ｝Ksl および｛Ks２´｝Ks１がメモリカード１１０から出力される（ステップＳ３４４）。

データバス BS３に出力された暗号データ｛受信ログ｝Ksl および｛Ks２´｝Ks１は、データバス BS３から端子１２０２およびメモリインタフェース１２００を介して携帯電話機１００に送信され、携帯電話機１００から配信サーバ３０に送信される（ステップＳ３４６）。

配信サーバ３０は、暗号化データ｛受信ログ｝Ksl および｛Ks２´｝Ks１を受信して、復号処理部３２０においてセッションキーKs１による復号処理を実行し、受信ログおよびメモリカードで生成されたセッションキーKs２´を受理する（ステップＳ３４８）。

続いて、配信制御部３１５は、受理した受信ログの正当性のチェックを行なう（ステップＳ３５０）。

受信ログが正当でないと判断されると、第２の再接続処理は終了する（ステップＳ３９０）。

一方、受信ログが正当であると判断されると、配信制御部３１５は、ライセンス配信ログからコンテンツ ID、アクセス制限情報 AC1、再生回路制限情報 AC2、および公開暗号鍵 KPm(1)を取得する（ステップＳ３５２）。さらに、暗号化コンテンツデータを復号するためのライセンスキーKc を情報データベース３０４より取得する（ステップＳ３５４）。

配信制御部３１５は、取得したライセンスキーKc および再生回路制限情報 AC２を暗号化処理部３２４に与える。暗号化処理部３２４は、Kcom 保持部３２２より得られる、秘密共通鍵 Kcom によって、ライセンスキーKc および再生回路制限情報 AC２を暗号化する（ステップＳ３５６）。

暗号化処理部３２４が出力する暗号化データ｛Kc//AC２｝Kcom と、配信制御部３１５が出力するトランザクション ID、コンテンツ ID およびアクセス制限情報 AC１とは、暗号化処理部３２６によって、ステップＳ３５２において得られたメモリカード１１０固有の公開暗号鍵 KPm（１）によって暗号化される（ステップＳ３５８）。

暗号化処理部３２８は、暗号化処理部３２６の出力を受けて、メモリカード１１０において生成されたセッションキーKs２´によって暗号化する（ステップＳ３６０）。

暗号化処理部３２８より出力された暗号化データ｛｛｛Kc//AC２｝Kcom//トランザクションＩＤ//コンテンツＩＤ//AC1｝Km(1)｝Ks2´は、データバス BS１および通信装置３５０を介して携帯電話機１００に送信される（ステップＳ３６２）。

携帯電話機１００は、送信された暗号化データ｛｛｛Kc//AC２｝Kcom//トランザクションＩＤ//コンテンツＩＤ//AC1｝Km(1)｝Ks2´を受信し（ステップＳ３６４）する。

図１２を参照して、メモリカード１１０においては、メモリインタフェース１２００を介して、データバス BS３に与えられた受信データを復号化処理部１４１２によって復号する。すなわち、復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーKs２´を用いてデータバス BS３の受信データを復号しデータバス BS４に出力する（ステップＳ３６６）。

この段階で、データバス BS４には、Km（１）保持部１４２１に保持される秘密復号鍵 Km（１）で復号可能なデータ｛｛Kc//AC２｝Kcom//ライセンスＩＤ//コンテンツＩＤ//AC1｝Km(1)が出力されている。このデータ｛｛Kc//AC２｝Kcom//トランザクションＩＤ//コンテンツＩＤ//AC1｝Km(1)が、まず秘密復号鍵 Km(1)により復号され、再生情報であるデータ｛Kc//AC２｝Kcom、トランザクシ

ョンＩＤ、コンテンツＩＤ、アクセス制限情報 ACl が受理される（ステップＳ３６８）。

トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報 ACl が、ライセンス情報保持部１４４０に記録される。データ {Kc//AC２} Kcom は、再び、秘密復号鍵 KPm(1)により暗号化され、データ { {Kc//AC２} Kcom} Km(1)としてメモリ１４１５に格納される（ステップＳ３７０）。

さらに、ログメモリ１４６０中の受信ログが消去される（ステップＳ３７２）。

ステップＳ３７２までの処理が正常に終了した段階で、携帯電話機１００から配信サーバ３０にコンテンツデータの配信要求がなされる（ステップＳ３７４）。

配信サーバ３０は、コンテンツデータの配信要求を受けて、情報データベース３０４より、暗号化コンテンツデータ {Data} Kc および付加情報 DATA-inf を取得して、これらのデータをデータバス BS１および通信装置３５０を介して出力する（ステップＳ３７６）。

携帯電話機１００は、{Data} Kc//Data-inf を受信して、暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf を受理する（ステップＳ３７８）。暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf はメモリインタフェース１２００および端子１２０２を介してメモリカード１１０のデータバス BS３に伝達される。メモリカード１１０においては、受信した暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf がそのままメモリ１４１５に格納される（ステップＳ３８０）。

さらに、メモリカード１１０から配信サーバ３０へは、配信受理の通知が送信され（ステップＳ３８２）、配信サーバ３０で配信受理を受信すると（ステップＳ３８４）、配信終了の処理が実行され（ステップＳ３８６）、配信サーバの処理が終了する（ステップＳ３９０）。

［第３の再接続処理］

図１３は、実施例１に従うデータ配信システムにおける、上述した第３の再接続動作を説明するためのフローチャートである。

図１３を参照して、ユーザ１が、携帯電話機１００のキーボード１１０８のキーボタンの操作等によって、再接続リクエストがなされ、これに応じて第３の再

接続処理が開始される（ステップＳ４００）。

携帯電話機１００においては、この再接続リクエストに応じて、配信サーバ３０にコンテンツデータの配信要求がなされる（ステップＳ４０２）。

配信サーバ３０は、コンテンツデータの配信要求を受けて、情報データベース３０４より、暗号化コンテンツデータ {Data} Kc および付加情報 DATA-inf を取得して、これらのデータをデータバス BS１および通信装置３５０を介して出力する（ステップＳ４０４）。

携帯電話機１００は、 {Data} Kc//Data-inf を受信して、暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf を受理する（ステップＳ４０６）。暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf はメモリインタフェース１２００および端子１２０２を介してメモリカード１１０のデータバスBS３に伝達される。メモリカード１１０においては、受信した暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf がそのままメモリ１４１５に格納される（ステップＳ４０８）。

さらに、メモリカード１１０から配信サーバ３０へは、配信受理の通知が送信され（ステップＳ４１０）、配信サーバ３０で配信受理を受信すると（ステップＳ４１２）、配信終了の処理が実行され（ステップＳ４１４）、配信サーバの処理が終了する（ステップＳ４１６）。

［再接続動作中に回線が切断した場合の再接続動作］

つづいて、以上説明した再接続動作のいずれか処理ステップの段階で、通信回線が途絶した場合に、さらに再度、配信を受けるために再接続が行なわれる場合の処理を説明する。図１４は、このような再接続処理を説明するためのフローチャートである。

まず、たとえば、ユーザ１が、携帯電話機１００のキーボード１１０８のキーボタンの操作等によって、再接続のリクエストがなされ、再接続処理が開始される（ステップＳ５００）。

つづいて、メモリカード１１０中に保持されたライセンス受信待ちログに基づいて、コントローラ１１０６は、通信が切断したステップが、いずれの処理中であったかを判断し（ステップＳ５０２）、それがライセンス取得ステップまたは

再ライセンス取得ステップであれば、第２の再接続処理を再度やり直し（ステップＳ５０４）、再接続処理が終了する（ステップＳ５０８）。

一方、コントローラ１１０６は、通信が切断したステップが、コンテンツデータ取得ステップであれば（ステップＳ５０２）、後に説明する第３の再接続処理を行ない（ステップＳ５０６）、再接続処理が終了する（ステップＳ５０８）。

このような構成とすることにより、いずれの処理ステップにおいて通信回線が途絶した場合でも、再接続を行なうことが可能で、システムの信頼性が一層強化される。

［実施例２］

実施例２のデータ配信システムにおいては、実施例１のデータ配信システムの構成と異なって、以下に説明するように、メモリカード１１０中のログメモリ１４６０に保持されたライセンス受信待ちログを消去しない点を特徴とする。このような変更を行なう結果、受信ログには、実施例１の構成に加えて、さらに、受信状態フラグが付け加わる構成となっている。

したがって、以下に説明するように実施例２のデータ配信システムの構成は、メモリカード１１０中のコントローラ１４２０の動作およびログメモリ１４６０に保持されるデータが実施例１の場合と異なる。

図１５、図１６および図１７は、実施例２に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第１、第２および第３のフローチャートであり、実施例１の図６～８と対比される図である。

図１５～図１７においても、ユーザ１が、メモリカード１１０を用いることで、携帯電話機１００を介して配信サーバ３０から音楽データの配信を受ける場合の動作を説明している。

実施例１のフローと異なる点は、トランザクションＩＤ取得ステップの後に、図１６に示した、ステップＳ１２１´では、コントローラ１４２０は、配信サーバ３０で生成されたセッションキーKs１の受理を確認すると、セッションキー発生部１４１８に対して、メモリカードにおいて配信動作時に生成されるセッションキーKs２の生成を指示する。さらに、コントローラ１４２０は、セッションキーKs２、受け取ったトランザクション ID とともに、受信待ちを示すオン状態と

なった受信状態フラグを受信ログとして、ログメモリ１４６０に記録する（ステップＳ１２１´）。

また、図１７を参照して、ステップＳ１４８において、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報 AC1 が、ライセンス情報保持部１４４０に記録される。データ｛Kc//AC２｝Kcom は、再び、公開暗号鍵 KPm(1)により暗号化され、データ｛｛Kc//AC２｝Kcom｝Km(1)としてメモリ１４１５に格納された後、ログメモリ１４６０中の受信ログ中の受信状態フラグは受信済みを示すオフ状態とされる（ステップＳ１５０´）。

その他の処理は、実施例１と同様であるので、同一処理には同一符号を付して、その説明は繰り返さない。

［再接続動作］

実施例２においても、実施例１の図９と同様に、以上説明した配信動作のいずれか処理ステップの段階で、通信回線が途絶した場合に、再度、配信を受けるために再接続処理が行なわれる。

ただし、実施例１の場合の第２の再接続処理の一部に変更が生じる。

［第２の再接続処理］

図１８、図１９および図２０は、実施例２に従うデータ配信システムにおける、上述した第２の再接続動作を説明するための第１、第２および第３のフローチャートであり、実施例１の図１０～図１２と対比される図である。

実施例１の処理と異なる点は、図１８において、ステップＳ３１８においてセッションキーＫｓ１を受理した後は、図１６に示したステップＳ１２１´に処理が移行する構成となっている点と、図２０において、ステップＳ３７０において、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報 AC1 が、ライセンス情報保持部１４４０に記録される。データ｛Kc//AC２｝Kcom は、再び、公開暗号鍵 KPm(1)により暗号化され、データ｛｛Kc//AC２｝Kcom｝Km(1)としてメモリ１４１５に格納した後、ステップＳ３７２´において、受信ログの受信状態フラグを受信済みを示すオフ状態とする処理を行なう構成となっている点である。

その他の処理は、実施例１と同様であるので、同一処理には同一符号を付して、その説明は繰り返さない。

さらに、第３の再接続処理や、再接続動作中に回線が切断した場合の再接続動作については、実施例１の処理と同様である。

以上のような構成とすることでも、いずれの処理ステップにおいて通信回線が途絶した場合でも、再接続を行なうことが可能で、システムの信頼性が一層強化される。

［実施例３］

実施例３のデータ配信システムにおいては、実施例２のデータ配信システムの構成と異なって、以下に説明するように、メモリカード１１０中のログメモリ１４６０に保持する受信ログに、状態フラグを加えた状態情報をサーバに送信する構成となっている点である。

状態情報は、受信ログであるトランザクションＩＤ、セッションキーＫｓ２、受信状態フラグと状態フラグという情報を含む。

ここで、ライセンス状態フラグは、３状態をとるフラグ変数であり、メモリカード１１０中のライセンス情報保持部１４４０に受信ログに記録されたトランザクションＩＤが存在し、対応する再生情報が存在し、かつ、ライセンス情報保持部１４４０に保持されるアクセス制限情報によって再生が禁止されていない、すなわち、再生可能な場合は、「０１ｈ」という値をとり、ライセンス情報保持部にトランザクションＩＤが存在し、対応する再生情報が無いか、ライセンス情報保持部１４４０に保持されるアクセス制限情報によって再生が禁止されていて再生できない場合には、「００ｈ」という値をとり、トランザクションＩＤが存在しない場合には、「ＦＦｈ」という値をとる。

したがって、以下に説明するように実施例３のデータ配信システムの構成は、メモリカード１１０中のコントローラ１４２０の動作およびログメモリ１４６０に保持されるデータが実施例２の場合と異なる。

実施例３の配信動作および再接続動作は、以下に説明する第２の再接続処理を除いては、実施例２の処理と同様であるので、その説明は繰り返さない。

［第２の再接続処理］

図２１、図２２、図２３および図２４は、実施例３に従うデータ配信システムにおける、第２の再接続動作を説明するための第１、第２、第３および第４のフ

ローチャートである。

まず、図２１を参照して、ステップＳ３００からステップＳ３３８までは、実施例２の第２の再接続動作と同様である。

ステップＳ３３８において、メモリカード１１０において、メモリインタフェース１２００を介して、データバス BS3に与えられた受信データを、復号処理部１４０４が、保持部１４０２に保持されるメモリカード１１０固有の秘密復号鍵 Kmc（1）により復号処理することにより、セッションキーKs1を復号し抽出した後、メモリカード１１０中のコントローラ１４２０は、ログメモリ１４６０中に保持された受信ログ中のトランザクションＩＤに従って、ライセンス情報保持部１４４０中に格納されているデータの検索を行なう（ステップ６４０）。

コントローラ１４２０は、まず、ライセンス情報保持部１４４０にトランザクションＩＤが存在するかをチェックする（ステップＳ６４２）。

トランザクションＩＤが存在しない場合、ライセンス状態フラグを「ＦＦｈ」に設定し（ステップＳ６４４）、処理はステップＳ６５２へ移行する。

一方、ステップＳ６４２において、トランザクションＩＤが存在する場合、さらに、コントローラ１４２０は、ライセンス情報保持部１４４０に保持されたアクセス制限情報ＡＣ１の状態やメモリ１４１５内に対応するライセンスキーＫｃが記録されているか否かを確認する（ステップＳ６４６）。再生が可能な場合はライセンス状態フラグを「０１ｈ」に設定する（ステップＳ６４８）。一方、再生できない場合は、ライセンス状態フラグを「００ｈ」に設定する（ステップＳ６５０）。その上で、処理はステップＳ６５２へ移行する。

続いて、ログメモリ１４６０の保持されている受信ログに状態フラグを付加した状態情報を生成する（ステップＳ６５２）。

コントローラ１４２０は、セッションキー発生部１４１８に対して、メモリカードにおいて配信動作時に生成されるセッションキーKs２´の生成を指示する（ステップＳ６５４）。

暗号化処理回路１４０６は、状態情報とセッションキーＫｓ２’をセッションキーＫｓ１で暗号化し、暗号化データ｛状態情報//Ｋｓ２’｝Ｋｓ１を生成する（ステップＳ６５６）。

コントローラ１４２０は、暗号化データ｛状態情報//Ｋｓ２'｝Ｋｓ１に対するハッシュ関数にしたがったハッシュ値を求め、暗号化データ｛状態情報//Ｋｓ２'｝Ｋｓ１に対する署名データｈａｓｈを生成する（ステップＳ６５８）。

暗号化処理部１４０６は、切換スイッチ１４４２の接点 Pa を介して復号処理部１４０４より与えられるセッションキーKs１によって、コントローラ１４２０の制御のもと与えられる署名データｈａｓｈを暗号化して暗号化署名データ｛hash｝Ks1 を生成する（ステップＳ６６０）。

以上のようにして生成されたデータ｛状態情報//Ｋｓ２'｝Ｋｓ１および暗号化署名データ｛hash｝Ks1 がメモリカード１１０から出力される（ステップＳ６６２）。

データバス BS３に出力された暗号データ｛状態情報//Ｋｓ２'｝Ｋｓ１および暗号化署名データ｛hash｝Ks1 は、データバス BS３から端子１２０２およびメモリインタフェース１２００を介して携帯電話機１００に送信され、携帯電話機１００から配信サーバ３０に送信される（ステップＳ６６４）。

配信サーバ３０は、暗号化データ｛状態情報//Ｋｓ２'｝Ｋｓ１および暗号化署名データ｛hash｝Ks1 を受信する（ステップＳ６６６）。

図２３を参照して、配信サーバ３０の復号処理部３２０において暗号化署名データ｛hash｝Ks1 に対してセッションキーKs１による復号処理を実行し、暗号データ｛状態情報//Ｋｓ２'｝Ｋｓ１に対する署名データｈａｓｈを得る。続いて、暗号データ｛状態情報//Ｋｓ２'｝Ｋｓ１と署名データから、状態情報の正当性をチェックする（ステップＳ６６８）。

状態情報が正当でないならば処理は終了し（ステップＳ７１２）、状態情報が正当であると確認されると、セッションキーKs１による復号処理を実行し、状態情報およびメモリカードで生成されたセッションキーKS２´を受理する（ステップS６７０）。

続いて、配信制御部３１５は、受理した状態情報とライセンス配信ログに基づいて再生情報の再送要求の正当性のチェックを行なう（ステップＳ６７２）。

再生情報の再送要求が正当でないと判断されると、第２の再接続処理は終了する（ステップＳ７１２）。

一方、再生情報の再送要求が正当であると判断されると、配信制御部３１５は、ライセンス配信ログからコンテンツ ID、アクセス制限情報 AC1、再生回路制限情報 AC2、および公開暗号鍵 KPm(1)を取得する（ステップＳ６７４）。さらに、暗号化コンテンツデータを復号するためのライセンスキーKc を情報データベース３０４より取得する（ステップＳ６７６）。

配信制御部３１５は、取得したライセンスキーKc および再生回路制限情報 AC２を暗号化処理部３２４に与える。暗号化処理部３２４は、Kcom 保持部３２２より得られる、秘密共通鍵 Kcom を用いて、ライセンスキーKc および再生回路制限情報 AC２を暗号化する（ステップＳ６７８）。

暗号化処理部３２４が出力する暗号化データ {Kc//AC２} Kcom と、配信制御部３１５が出力するトランザクション ID、コンテンツ ID およびアクセス制限情報 AC１とは、暗号化処理部３２６によって、ステップＳ６７４において得られたメモリカード１１０固有の公開暗号鍵 KPm（１）によって暗号化される（ステップＳ６８０）。

暗号化処理部３２８は、暗号化処理部３２６の出力を受けて、メモリカード１１０において生成されたセッションキーKs２´によって暗号化する（ステップＳ６８２）。

暗号化処理部３２８より出力された暗号化データ {{{Kc//AC２} Kcom//トランザクションＩＤ//コンテンツＩＤ//AC1} Km(1)} Ks2´は、データバス BS１および通信装置３５０を介して携帯電話機１００に送信される（ステップＳ６８４）。

携帯電話機１００は、送信された暗号化データ {{{Kc//AC２} Kcom//トランザクションＩＤ//コンテンツＩＤ//AC1} Km(1)} Ks2´を受信し（ステップＳ６８６）する。

図２４を参照して、メモリカード１１０においては、メモリインタフェース１２００を介して、データバス BS３に与えられた受信データを復号化処理部１４１２によって復号する。すなわち、復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーKs２´を用いてデータバス BS３の受信データを復号しデータバス BS４に出力する（ステップＳ６９０）。

この段階で、データバス BS４には、Km（１）保持部１４２１に保持される秘密復号鍵 Km（１）で復号可能なデータ｛｛Kc//AC２｝Kcom//ライセンスＩＤ//コンテンツＩＤ//AC1｝Km(1)が出力されている。このデータ｛｛Kc//AC２｝Kcom//トランザクションＩＤ//コンテンツＩＤ//AC1｝Km(1)が、まず公開暗号鍵 Km(1)により復号され、データ｛Kc//AC２｝Kcom、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報 AC1 が受理される（ステップＳ６９２）。

トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報 AC1 が、ライセンス情報保持部１４４０に記録される。データ｛Kc//AC２｝Kcom は、再び、公開暗号鍵 KPm(1)により暗号化され、データ｛｛Kc//AC２｝Kcom｝Km(1)としてメモリ１４１５に格納される（ステップＳ６９４）。

さらに、ログメモリ１４６０中の受信ログ中の受信状態フラグ受信済みを示すオフ状態に変更される（ステップＳ６９６）。

ステップＳ３７２までの処理が正常に終了した段階で、携帯電話機１００から配信サーバ３０にコンテンツデータの配信要求がなされる（ステップＳ６９８）。

配信サーバ３０は、コンテンツデータの配信要求を受けて、情報データベース３０４より、暗号化コンテンツデータ｛Data｝Kc および付加情報 DATA-inf を取得して、これらのデータをデータバス BS１および通信装置３５０を介して出力する（ステップＳ７００）。

携帯電話機１００は、｛Data｝Kc//Data-inf を受信して、暗号化コンテンツデータ｛Data｝Kc および付加情報 Data-inf を受理する（ステップＳ７０２）。暗号化コンテンツデータ｛Data｝Kc および付加情報 Data-inf はメモリインタフェース１２００および端子１２０２を介してメモリカード１１０のデータバス BS３に伝達される。メモリカード１１０においては、受信した暗号化コンテンツデータ｛Data｝Kc および付加情報 Data-inf がそのままメモリ１４１５に格納される（ステップＳ７０４）。

さらに、メモリカード１１０から配信サーバ３０へは、配信受理の通知が送信され（ステップＳ７０６）、配信サーバ３０で配信受理を受信すると（ステップＳ７０８）、配信終了の処理が実行され（ステップＳ７１０）、配信サーバの処理が終了する（ステップＳ７１２）。

なお、以上の説明では、ステップＳ６５４において、状態情報の全ての情報をセッションキーＫｓ１で暗号化して、ステップＳ６２２およびＳ６２４により、配信サーバ３０に対して、暗号化データ｛状態情報//Ｋｓ２'｝Ｋｓ１が送信される構成となっている。

しかしながら、状態情報のうちトランザクションＩＤについては、その機密というよりは、その出所が明らかであれば良い情報である。したがって、暗号化署名データ｛hash｝Ksl によって、その出所が明らかとなるので、このトランザクションＩＤについては暗号化せず、平文のままで配信サーバ３０に送信される構成でもよい。この場合、状態情報は、トランザクションＩＤ//｛トランザクションＩＤを除く状態情報//Ｋｓ２'｝Ｋｓ１として送信されることとなり、署名データｈａｓｈはこれに対して生成される。

以上のような構成とすることでも、いずれの処理ステップにおいて通信回線が途絶した場合でも、再接続を行なうことが可能で、システムの信頼性が一層強化される。

さらに、実施例１～３のデータ配信システムでは、配信サーバ３０および携帯電話機１００において秘密共通鍵 Kcom による暗号化および復号処理が行なわれる構成となっていたが、この秘密共通鍵 Kcom による暗号化および復号処理を用いない構成とすることも可能である。

すなわち、図３において説明した、実施例１のデータ配信システムが具備する配信サーバ３０において、Kcom 保持部３２２と暗号化処理部３２４を具備しない構成とすることが可能である。すなわち、このような配信サーバ３０においては、配信制御部３１５が出力するライセンスキーKc および再生回路制限情報 AC２は、直接暗号化処理部３２６に伝達される。

さらに、実施例１の図４で説明した携帯電話機１００の構成と比較して、秘密共通鍵 Kcom を保持する Kcom 保持部１５１２と秘密共通鍵 Kcom による復号処理部１５１４を具備しない構成とすることが可能である。

すなわち、このような構成の携帯電話機１０１においては、配信サーバ３０において秘密共通鍵を対称な暗号鍵として暗号化処理が施されていないことに対応して、セッションキーKs４による復号処理を実行する復号処理部１５１０によっ

て直接ライセンスキーKc.が得られるため、これを復号処理部１５１０に直接与える構成となる。

また、このように秘密共通鍵 Kcom による暗号化および復号処理を用いない構成においても、メモリカード１１０はそのまま用いることができる。

このような場合の配信処理等では、コンテンツキーＫｃや再生回路制限情報ＡＣ２が秘密復号鍵 Kcom により暗号化されずに伝送され保持され、また、秘密復号鍵Kcomによる暗号化処理および対応する復号処理が不要となる点を除いては、実施例１～３の動作と同様である。

このような構成とすることによって、秘密共通鍵Kcomに関する暗号化処理を行なわないような構成としても、実施例１～３に従うデータ配信システムと同様の効果を享受するデータ配信システムを構築することが可能である。

さらに、以上説明した実施例１～３において、以下のような変更を行うことも可能である。

まず、実施例１～３においては、データ｛Ｋｃ//ＡＣ２｝Kcom（または、上述したように鍵Kcomを省略する構成では、データＫｃ//ＡＣ２）を、公開暗号鍵ＫＰｍ（１）により再暗号化した上で、ライセンス情報保持部１４４０に記録する構成としていた。しかしながら、ＴＲＭ内に設けられるライセンス情報保持部１４４０に格納されるのであれば、必ずしも、公開暗号鍵ＫＰｍ（１）による再暗号化を行う必要はなく、再生情報の全てをライセンス情報保持部１４４０に記録するものとしても、実施例１～３と同様の効果が奏される。この場合、実施例１では、図８におけるステップＳ１４８、図１２におけるステップＳ３７０を、「トランザクションＩＤ、コンテンツＩＤ、ＡＣ１、｛Ｋｃ//ＡＣ２｝Kcomをライセンス情報保持部に記録する」と変更すればよい。また、実施例２では、図１７におけるステップＳ１４８、図２０におけるステップＳ３７０を、実施例３では、図２４におけるステップＳ６９４も、実施例１と同様に、「トランザクションＩＤ、コンテンツＩＤ、ＡＣ１、｛Ｋｃ//ＡＣ２｝Kcomをライセンス情報保持部に記録する」と変更すればよい。さらに、上記実施例１～３のいずれの変更に対しても、鍵Kcomを省略する構成とするのであれば、「トランザクションＩＤ、コンテンツＩＤ、ＡＣ１、Ｋｃ//ＡＣ２をライセンス情報保持部に記録する」と

変更すればよい。

さらに、すべての実施例１～３のデータ配信システムでは配信サーバから再生情報の配信を受けるにあたって、メモリカードおよび携帯電話機（コンテンツ再生回路）の認証データ｛ＫＰｍ（１）｝ＫＰｍａおよび｛ＫＰｐ（１）｝ＫＰｍａを、配信サーバに送信し（ステップＳ１０４）、配信サーバは受信（ステップＳ１０６）し、認証鍵ＫＰｍａにて復号（ステップＳ１０８）後、復号結果に従って、メモリカードと携帯電話機（コンテンツ再生回路）の双方に対する認証処理をするよう説明した。しかしながら、ｉ）メモリカードは挿脱可能であることから、音楽を再生するのにコンテンツ再生回路が必ずしも配信を受けた携帯電話機である必然性がないこと、ｉｉ）再生に際して、メモリカード内においても、再生情報の一部（ライセンスキーＫｃおよび再生回路制限情報ＡＣ２）を出力するにあたって、出力先のコンテンツ再生回路の認証データ｛ＫＰｍ（１）｝ＫＰｍａの認証処理を行っており、配信サーバにおけるコンテンツ再生回路の認証データ｛ＫＰｍ（１）｝ＫＰｍａの認証処理を行わなくてもセキュリティの低下につながらないことの２点から、配信サーバにおけるコンテンツ再生回路の認証データ｛ＫＰｍ（１）｝ＫＰｍａの認証処理を行わない構成にしてもよい。

この場合、携帯電話機は、ステップＳ１０４にて、コンテンツＩＤとメモリカードの認証データ｛ＫＰｍ（１）｝ＫＰｍａおよびライセンス購入条件データＡＣを送信し、配信サーバは、ステップＳ１０６にて、コンテンツＩＤとメモリカードの認証データ｛ＫＰｍ（１）｝ＫＰｍａおよびライセンス購入条件データＡＣを送信し、ステップＳ１０８にて、認証データ｛ＫＰｍ（１）｝ＫＰｍａを認証鍵ＫＰｍａにて復号して公開暗号鍵ＫＰｍ（１）を受理する。続いて、ステップＳ１１０にて、復号結果に基づいて、あるいは認証サーバに問い合わせて、公開暗号鍵ＫＰｍ（１）が正当な機器から出力されたものか否かを判断する認証処理を行い、メモリカードの認証データ｛ＫＰｍ（１）｝ＫＰｍａの認証結果に従い、以降の処理を行うように変更するのみでよく、再生処理は何ら変更はない。

また、以上の説明では、配信された情報の格納は、メモリカードにより行われるものとしたが、本発明はこのような場合に限定されるものではない。すなわち、以上説明したようなメモリカードと同様の記録および暗号化などの機能を有する

のであれば、より一般的な記録装置にも適用可能である。このとき、記録装置は、携帯電話機のような通信装置にメモリカードのように着脱可能である構成にも必ずしも限定されず、通信装置に組み込まれる構成とすることも可能である。

この発明を詳細に説明し示してきたが、これは例示のためのみであって、限定となってはならず、発明の精神と範囲は添付の請求の範囲によってのみ限定されることが明らかに理解されるであろう。

請求の範囲

１．暗号化コンテンツデータの再生に関連し、前記暗号化コンテンツデータを復号して平文にするためのコンテンツキーを含む再生情報を、通信経路を介して受けて記録するためのメモリカード（１１０）であって、

暗号化されて送られる前記再生情報の受信のために、前記再生情報の送信元との間での通信経路を確立するためのデータ通信部と、

前記データ通信部から与えられる前記再生情報に関連するデータを保持するための第１の記憶部（１４１５，１４４０）と、

前記データ通信部からの前記再生情報に関連するデータを前記第１の記憶部へ格納する処理を行い、かつ前記第１の記憶部に格納されたデータに基づいて、前記再生情報を抽出するための情報抽出部と、

前記再生情報の送信処理における処理状態を示す受信ログ情報を記録するための第２の記憶部（１４６０）と、

前記メモリカードの動作を制御するための制御部（１４２０）とを備え、

前記制御部は、要求に応じて前記受信ログ情報の前記送信元への送信を制御するメモリカード。

２．前記データ通信部は、

前記メモリカードに対応して予め定められた第１の公開暗号鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第１の鍵保持部（１４０２）と、

前記再生情報の通信ごとに更新されて送信され、前記第１の公開暗号鍵によって暗号化された第１の共通鍵を受けて、復号処理するための第１の復号処理部（１４０４）と、

前記メモリカードごとに異なる第２の公開暗号鍵を保持するための第２の鍵保持部（１４１６）と、

前記再生情報の通信ごとに更新して第２の共通鍵を生成する鍵生成部（１４１８）と、

前記第２の公開暗号鍵および前記第２の共通鍵を、前記第１の共通鍵に基づい

て暗号化し、出力するための第１の暗号化処理部（１４０６）と、

前記第２の公開暗号鍵で暗号化され、さらに前記第２の共通鍵で暗号化された前記再生情報を受け、前記第２の共通鍵に基づいて復号するための第２の復号処理部（１４１２）とを含み、

前記第１の記憶部は、前記第２の復号処理部の出力に基づいたデータを保持し、

前記情報抽出部は、

前記第２の公開暗号鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する第３の鍵保持部（１４２１）と、

前記再生情報に関連するデータの前記第１の記憶部への格納処理から前記再生情報を抽出する処理までの過程において、前記第２の秘密復号鍵についての復号処理を行なう第３の復号処理部（１４２２）とを含む、請求項１記載のメモリカード。

３．前記第１の記憶部は、

前記再生情報のうち前記コンテンツキーを含む一部である第１のデータを暗号化した状態で格納するための第３の記憶部（１４１５）と、

前記再生情報のうちの前記一部のデータを除く第２のデータを平文の状態で格納するための第４の記憶部（１４４０）とを含み、

前記情報抽出部は、前記第３の復号処理部が前記第２の復号処理部の出力に対して復号処理を行なった結果のうち、前記第２のデータを前記第４の記憶部に格納し、かつ

前記第３の復号処理部が前記第２の復号処理部の出力に対して復号処理を行なった結果のうちの一部を前記第２の公開暗号鍵で再び暗号化して、前記第３の記憶部に格納されるべき前記第１のデータを生成するための再暗号化処理部を含む、請求項２記載のメモリカード。

４．前記第３の記憶部は、前記コンテンツキーに基づいて復号できる前記暗号化コンテンツデータを受けて格納する、請求項３記載のメモリカード。

５．前記情報抽出部は、前記第３の復号処理部が前記第２の復号処理部の出力に対して復号処理を行なった結果を、平文の状態で前記第１の記憶部に格納する、請求項２記載のメモリカード。

6．前記第１の記憶部は、

前記コンテンツキーに基づいて復号できる前記暗号化コンテンツデータを受けて格納するための第３の記憶部（１４１５）と、

前記再生情報を平文の状態で格納するための第４の記憶部（１４４０）とを含む、請求項５記載のメモリカード。

7．前記メモリカードは、

前記再生情報の送信に先だって、前記再生情報の送信元にて認証処理を行なうための認証データを保持する第５の記憶部（１４００）をさらに備え、

前記受信ログ情報は、前記認証処理において前記メモリカードが認証された場合において、前記送信元から送信される前記再生情報の送信が行なわれるごとに前記送信元で生成され、前記送信を特定するための通信特定情報と、前記第２の共通鍵とを有する、請求項２記載のメモリカード。

8．前記メモリカードは、

前記再生情報の送信に先だって、前記再生情報の送信元にて認証処理を行なうための認証データを保持する第５の記憶部（１４００）をさらに備え、

前記受信ログ情報は、

前記認証処理において前記メモリカードが認証された場合において、前記送信元から送信される前記再生情報の送信が行なわれるごとに前記送信元で生成され、前記送信を特定するための通信特定情報と、

受信済みの前記再生情報の状態を示す状態情報と、

前記第２の共通鍵とを有し、

少なくとも前記状態情報と前記第２の共通鍵とに基づく署名情報を生成して出力する手段をさらに備える、請求項２記載のメモリカード。

9．前記第１の暗号化処理部は、前記受信ログ情報と前記署名情報とをそれぞれ前記第１の共通鍵に基づいて暗号化し、

前記メモリカードは、前記第１の暗号化処理部で個別に暗号化された前記受信ログ情報と前記署名情報とを前記送信元に返信する、請求項８記載のメモリカード。

１０．前記受信ログ情報は、前記コンテンツキーが前記第１の記憶部に格納され

るごとに、前記第２の記憶部から消去される、請求項１記載のメモリカード。

１１．前記受信ログ情報は、前記コンテンツキーの送信を前記送信元に対して要求するごとにオン状態とされ、前記コンテンツキーが前記第１の記憶部に格納されるごとに、オフ状態とされる受信状態フラグをさらに有する、請求項１記載のメモリカード。

１２．データ配信システムであって、

暗号化コンテンツデータと、暗号化コンテンツデータの再生に関連し、かつ前記暗号化コンテンツデータを復号して平文にするための復号鍵であるコンテンツキーを含む再生情報とを供給するためのコンテンツデータ供給装置を備え、

前記コンテンツデータ供給装置（１０）は、

前記コンテンツデータおよび前記再生情報を保持するための配信情報保持部（３０４）と、

外部との間でデータを授受するための第１のインタフェース部（３５０）と

前記端末に対する前記再生情報の配信ごとに更新される第１の共通鍵を生成する第１のセッションキー発生部（３１６）と、

前記ユーザの端末に対応して予め定められた第１の公開暗号鍵により前記第１の共通鍵を暗号化して前記第１のインタフェース部に与えるためのセッションキー暗号化部（３１８）と、

前記第１の共通鍵により暗号化されて返信される第２の公開暗号鍵と第２の共通鍵とを復号するためのセッションキー復号部（３２０）と、

前記暗号化コンテンツデータを再生するための再生情報を、前記セッションキー復号部により復号された前記第２の公開暗号鍵によって暗号化するための第１のライセンスデータ暗号処理部（３２６）と、

前記第１のライセンスデータ暗号処理部の出力を前記第２の共通鍵でさらに暗号化して前記第１のインタフェース部に与え配信するための第２のライセンスデータ暗号処理部（３２８）と、

前記配信処理中の処理状態を示す配信ログ情報を記録するための配信ログ情報保持部（３０６）とを含み、

前記コンテンツデータ供給装置から、通信経路を介して配信を受けるために複

数のユーザにそれぞれ対応する複数の端末（１００）をさらに備え、

各前記端末は、

外部との間でデータ授受をするための第２のインタフェース部（１１０４）と、

前記暗号化コンテンツデータと前記再生情報とを受けて格納するデータ格納部（１１０）とを含み、

前記データ格納部は、

前記データ格納部に対応して予め定められた第１の公開暗号鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第１の鍵保持部（１４０２）と、

前記再生情報の通信ごとに更新されて配信され、前記第１の公開暗号鍵によって暗号化された第１の共通鍵を受けて、復号処理するための第１の復号処理部（１４０４）と、

前記データ格納部ごとに異なる第２の公開暗号鍵を保持するための第２の鍵保持部（１４１６）と、

前記再生情報の通信ごとに更新して第２の共通鍵を生成する鍵生成部（１４１８）と、

前記第２の公開暗号鍵および前記第２の共通鍵を、前記第１の共通鍵に基づいて暗号化し、出力するための第１の暗号化処理部（１４０６）と、

前記第２の公開暗号鍵で暗号化され、さらに第２の共通鍵で暗号化された再生情報を受け、前記第２の共通鍵に基づいて復号するための第２の復号処理部（１４１２）と、

前記第２の復号処理部の出力に基づいたデータを保持する第１の記憶部（１４１５，１４４０）と、

前記第２の公開暗号鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する第３の鍵保持部（１４２１）と、

前記再生情報に関連するデータの前記第１の記憶部への格納処理から前記再生情報を抽出する処理までの過程において、前記第２の秘密復号鍵についての復号処理を行なう第３の復号処理部（１４２２）と、

前記暗号化コンテンツデータおよび前記再生情報の配信処理における処理状態

を示す受信ログ情報を記録するための第２の記憶部（１４６０）と、

外部との間のデータ授受を制御する受信制御部（１４２０）とを有し、

前記受信制御部は、前記配信処理中に前記通信経路が切断された場合に、前記受信ログ情報に基づいて再配信処理を制御する、データ配信システム。

１３．前記データ格納部は、前記端末に着脱可能なメモリカードである、請求項１２記載のデータ配信システム。

１４．前記コンテンツデータ供給装置は、

前記再生情報の配信に先だって、前記メモリカードから送信される認証データにより前記メモリカードを認証する手段（３１２）と、

前記再生情報の配信処理を行なうごとに、前記配信処理を特定するための配信特定情報を生成する手段（３１５）とをさらに備え

前記メモリカードは、

前記認証データを保持する第３の記憶部（１４６０）をさらに備え、

前記受信ログ情報は、前記認証処理において前記メモリカードが認証された場合において、送信元から送信される、前記再生情報の送信が行なわれるごとに前記送信元で生成され、前記送信を特定するための通信特定情報と前記第２の共通鍵とを有する、請求項１３記載のデータ配信システム。

１５．前記受信ログ情報は、前記再生情報が前記第１の記憶部に格納されるごとに、前記第２の記憶部から消去される、請求項１２記載のデータ配信システム。

１６．前記受信ログ情報は、前記再生情報の配信を前記送信元に対して要求するごとにオン状態とされ、前記再生情報が前記第１の記憶部に格納されるごとに、オフ状態とされる受信状態フラグを含む、請求項１２記載のデータ配信システム。

１７．前記受信ログ情報は、少なくとも前記通信特定情報と前記第２の共通鍵を有する、請求項１２記載のデータ配信システム。

FIG. 1

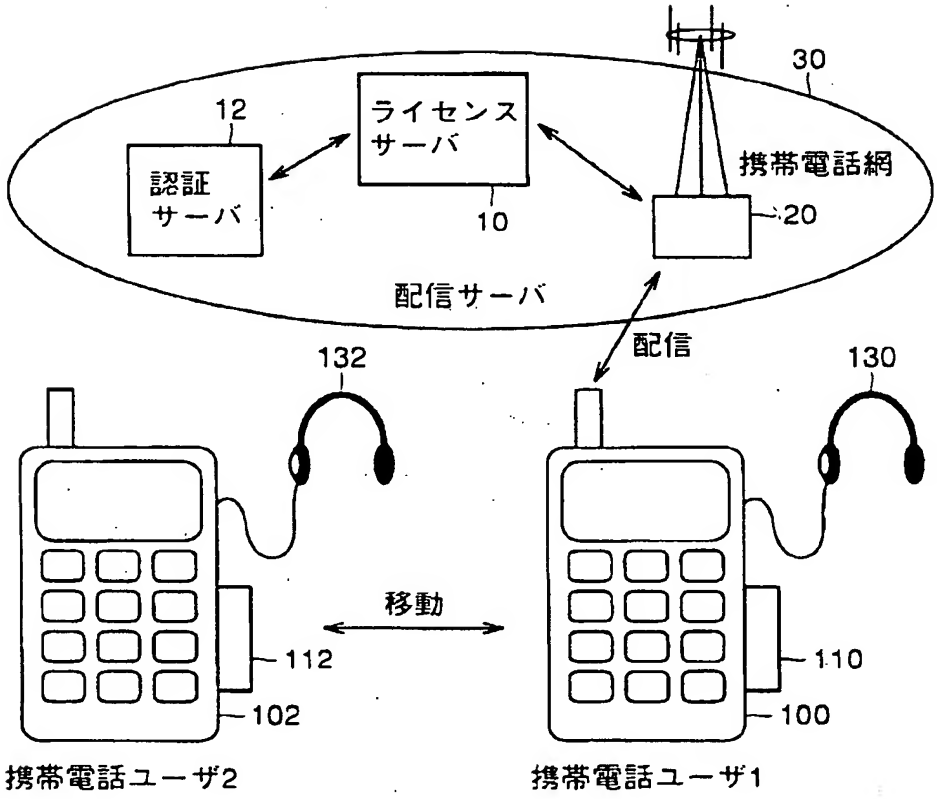

30
12
ライセンス
サーバ
認証
サーバ
10
携帯電話網
20
配信サーバ
配信
132
130
移動
112
110
102
100
携帯電話ユーザ2
携帯電話ユーザ1

FIG.2

名称	機能・特徴	保持・発生箇所
Data	コンテンツデータ、Kcにて復号可能な暗号化を施した暗号化コンテンツデータとして{Data}Kcの形式にて配布	配信サーバ
Data-inf	付加情報、コンテンツデータに関する著作関連あるいはサーバアクセス関連等の平文情報	配信サーバ
Kc	コンテンツ復号キー	配信サーバ
Kp(n)/Kmc(n)	コンテンツ再生／メディアのクラス(種類等)に依存する復号鍵	携帯電話機 メモリカード
KPp(n)/KPmc(n)	Kp/Kmcにて復号可能な非対称暗号化鍵、認証機能を有する。 {KPp}KPma/{KPp}KPmaの形式で出荷時に記録	携帯電話機 メモリカード
Kcom	再生回路共通の秘密復号鍵、暗号化されたKc,AC2の復号に利用 （非対称　配信サーバKPcom／再生回路Kcom　も良い）	配信サーバ 携帯電話機
KPma	システム共通の認証鍵(公開)	配信サーバ
AC	利用者側からのライセンスに対する購入条件(機能限定、ライセンス数etc)	携帯電話機
AC1	メモリのアクセスに対する制限情報	配信サーバ
AC2	再生回路における制御情報	配信サーバ
Km(i)	メモリカード毎に固有の復号鍵(iはカードを識別する識別子)	メモリカード
KPm(i)	Km(i)にて復号可能な非対称な公開暗号鍵	メモリカード
Ks1	配信セッション毎に発生するセッション固有の共通鍵	配信サーバ
Ks2	配信／移動(受)セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks3	再生セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks4	再生セッション毎に発生するセッション固有の共通鍵	携帯電話機
コンテンツID	コンテンツデータDataを識別するコード	配信サーバ
トランザクションID	ライセンスの発行を特定できる管理コード(コンテンツIDをも含めて識別することも考えられる)	配信サーバ

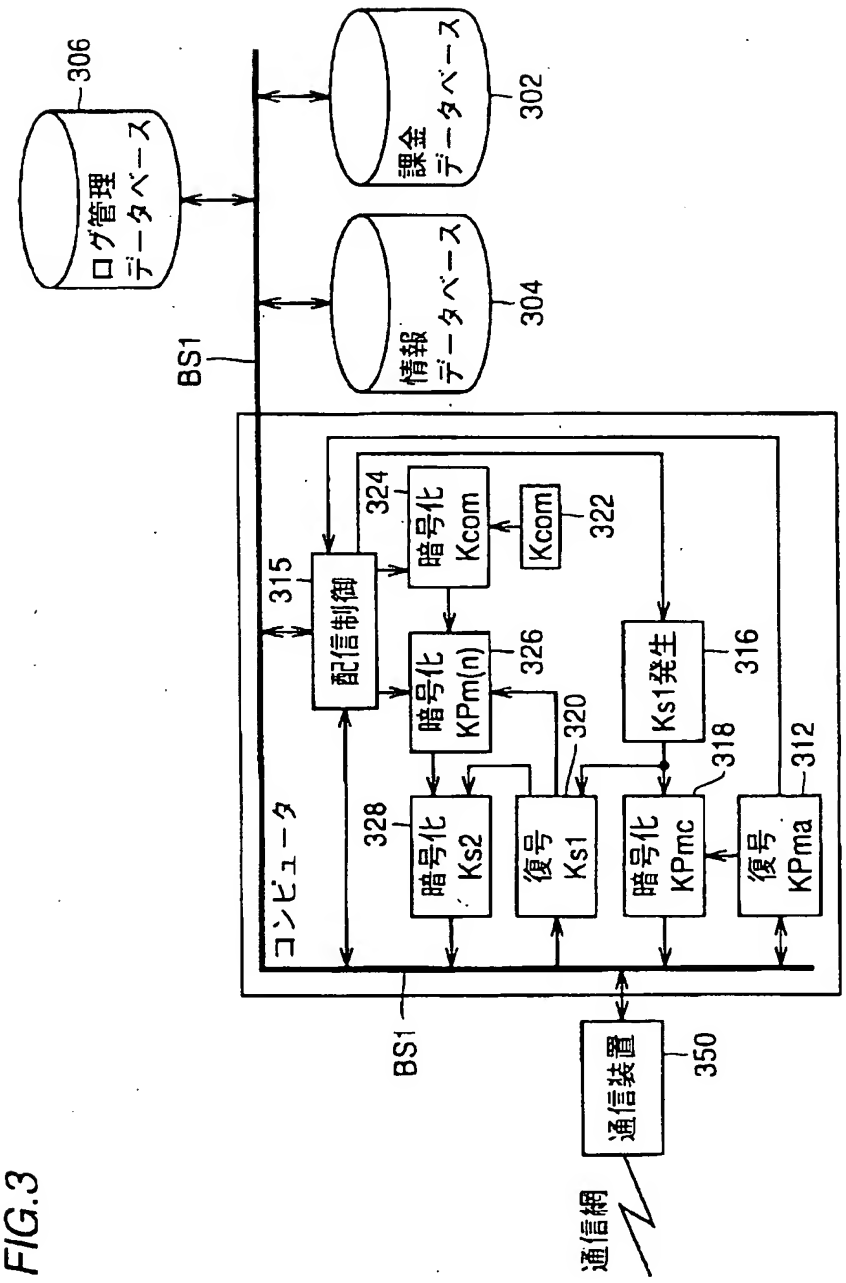

30
306
ログ管理データベース
302
課金データベース
304
情報データベース
BS1
コンピュータ
315
配信制御
324
暗号化 Kcom
Kcom
322
暗号化 KPm(n)
326
Ks1発生
316
320
318
328
暗号化 Ks2
復号 Ks1
暗号化 KPmc
復号 KPma
312
BS1
通信装置
350
通信網

FIG.3

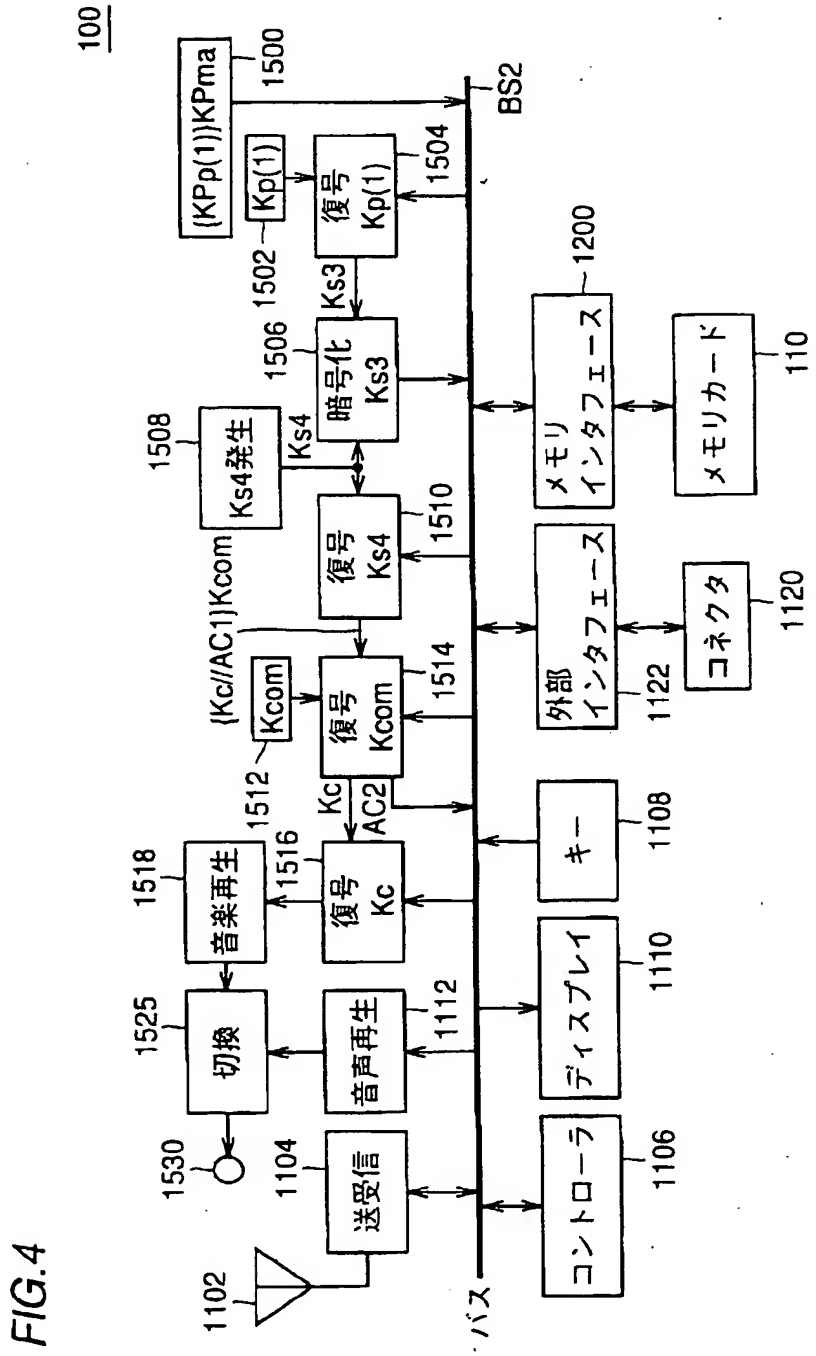

100
{KPp(1)}KPma
1500
BS2
Kp(1)
1502
復号 Kp(1)
1504
Ks3
1506
暗号化 Ks3
Ks4
1508
Ks4発生
復号 Ks4
1510
{Kc//AC1}Kcom
Kcom
復号 Kcom
1514
Kc
AC2
1512
音楽再生
1518
復号 Kc
1516
切換
1525
音声再生
1112
送受信
1104
1530
1102
バス
コントローラ
1106
ディスプレイ
1110
キー
1108
外部インタフェース
1122
メモリインタフェース
1200
コネクタ
1120
メモリカード
110

FIG.4

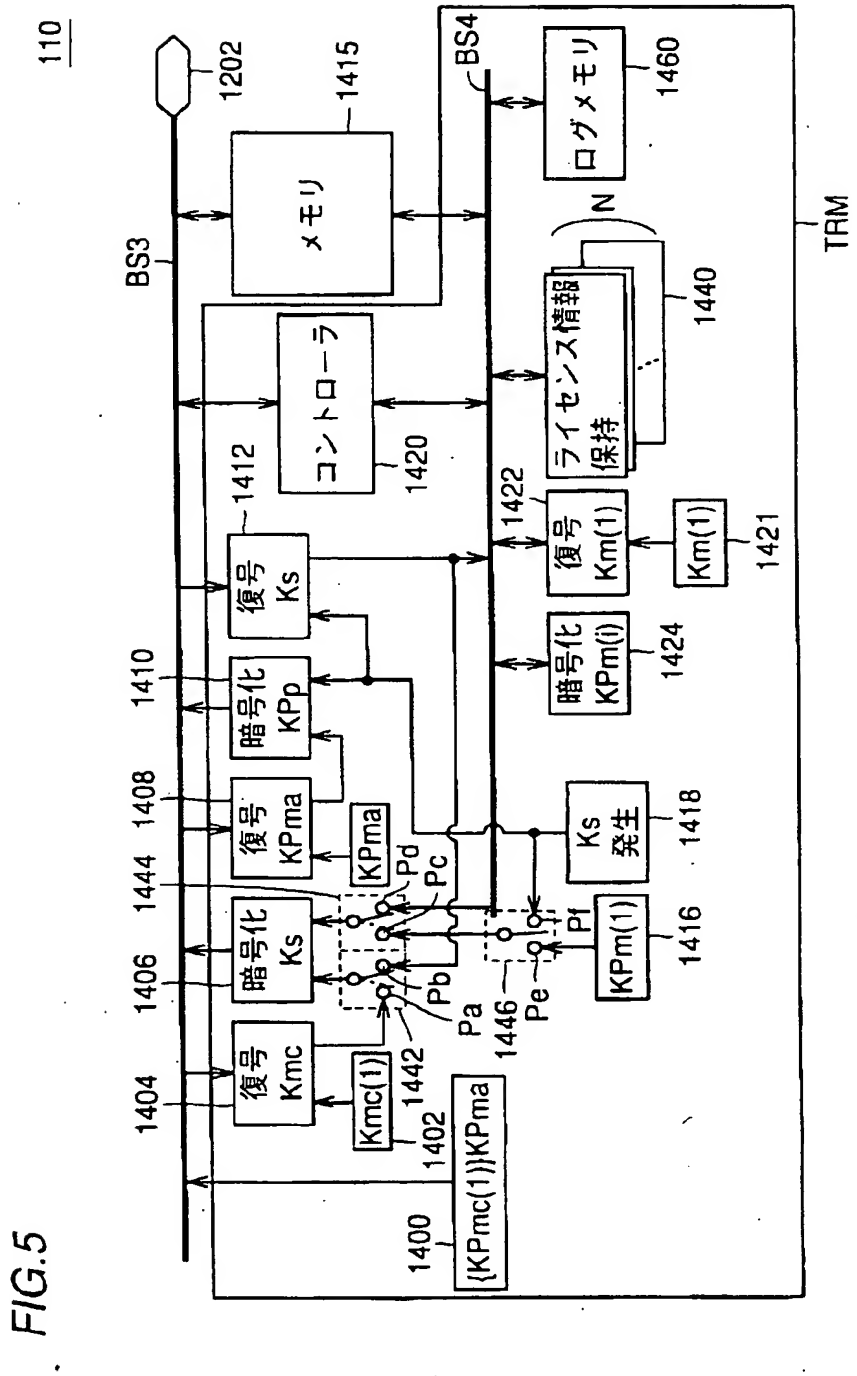

110
1202
1415
BS4
1460
ログメモリ
BS3
メモリ
TRM
N
1440
ライセンス情報保持
1412
コントローラ
1420
1422
復号 Km(1)
Km(1)
1421
復号 Ks
1410
暗号化 KPp
暗号化 KPm(i)
1424
1408
復号 KPma
KPma
Pd
Pc
Ks 発生
1418
1444
暗号化 Ks
Pf
1406
Pb
Pa
Pe
1446
KPm(1)
1416
1404
復号 Kmc
Kmc(1)
1442
1402
{KPmc(1)}KPma
1400

FIG.5

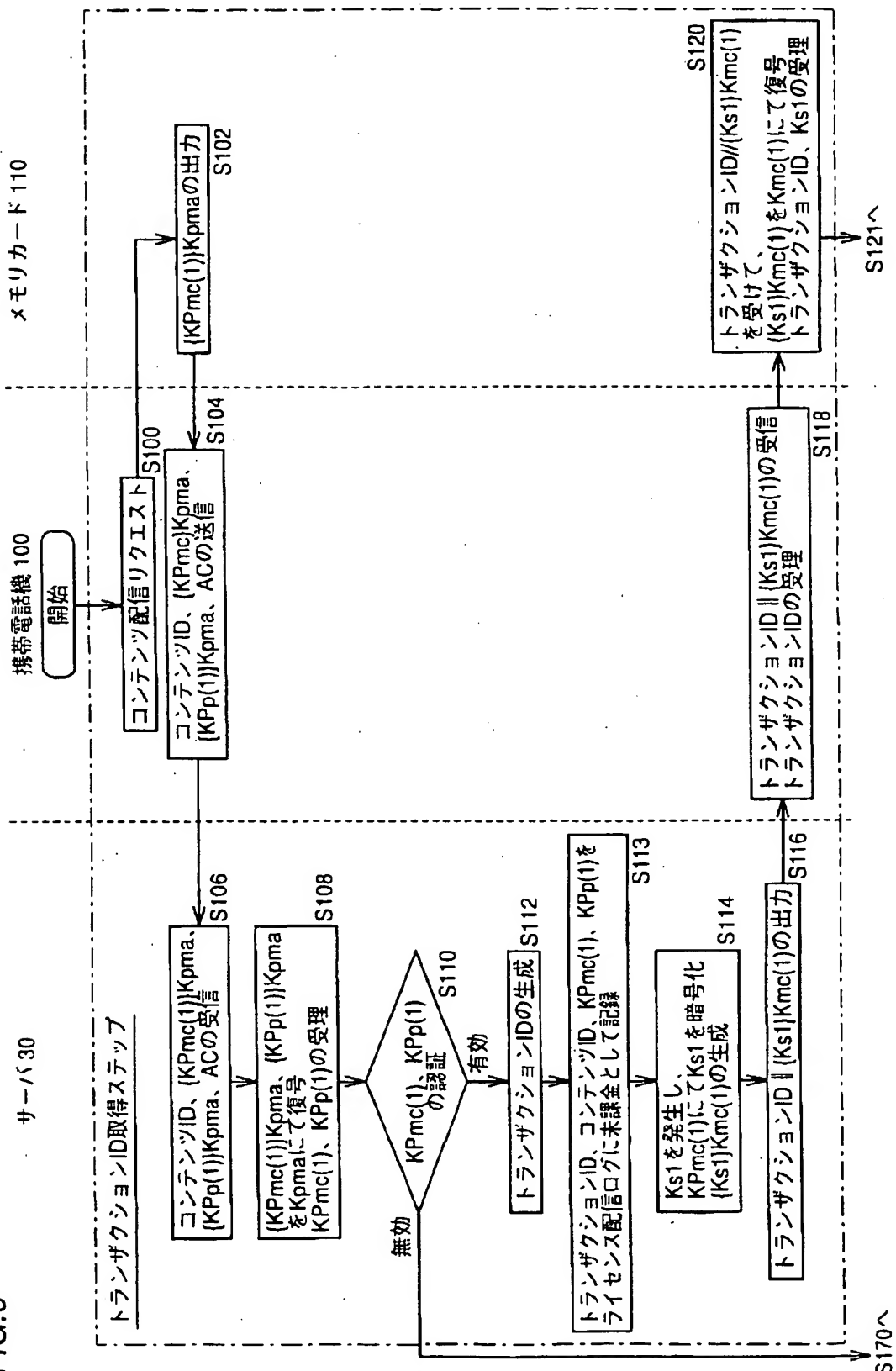

携帯電話機 100
開始
コンテンツ配信リクエスト
S100
メモリカード 110
{KPmc(1)}Kpmaの出力
S102
コンテンツID、{KPmc}Kpma、{KPp(1)}Kpma、ACの送信
S104
S120
トランザクションID//{Ks1}Kmc(1)を受けて、{Ks1}Kmc(1)をKmc(1)にて復号トランザクションID、Ks1の受理
S121へ
トランザクションID取得ステップ
サーバ 30
コンテンツID、{KPmc(1)}Kpma、{KPp(1)}Kpma、ACの受信
S106
{KPmc(1)}Kpma、{KPp(1)}KpmaをKpmaにて復号KPmc(1)、KPp(1)の受理
S108
KPmc(1)、KPp(1)の認証
S110
無効
有効
トランザクションIDの生成
S112
トランザクションID、コンテンツID、KPmc(1)、KPp(1)をライセンス配信ログに未課金として記録
S113
Ks1を発生し、KPmc(1)にてKs1を暗号化{Ks1}Kmc(1)の生成
S114
トランザクションID ‖ {Ks1}Kmc(1)の出力
S116
トランザクションID ‖ {Ks1}Kmc(1)の受信トランザクションIDの受理
S118
S170へ

FIG.6

FIG.7

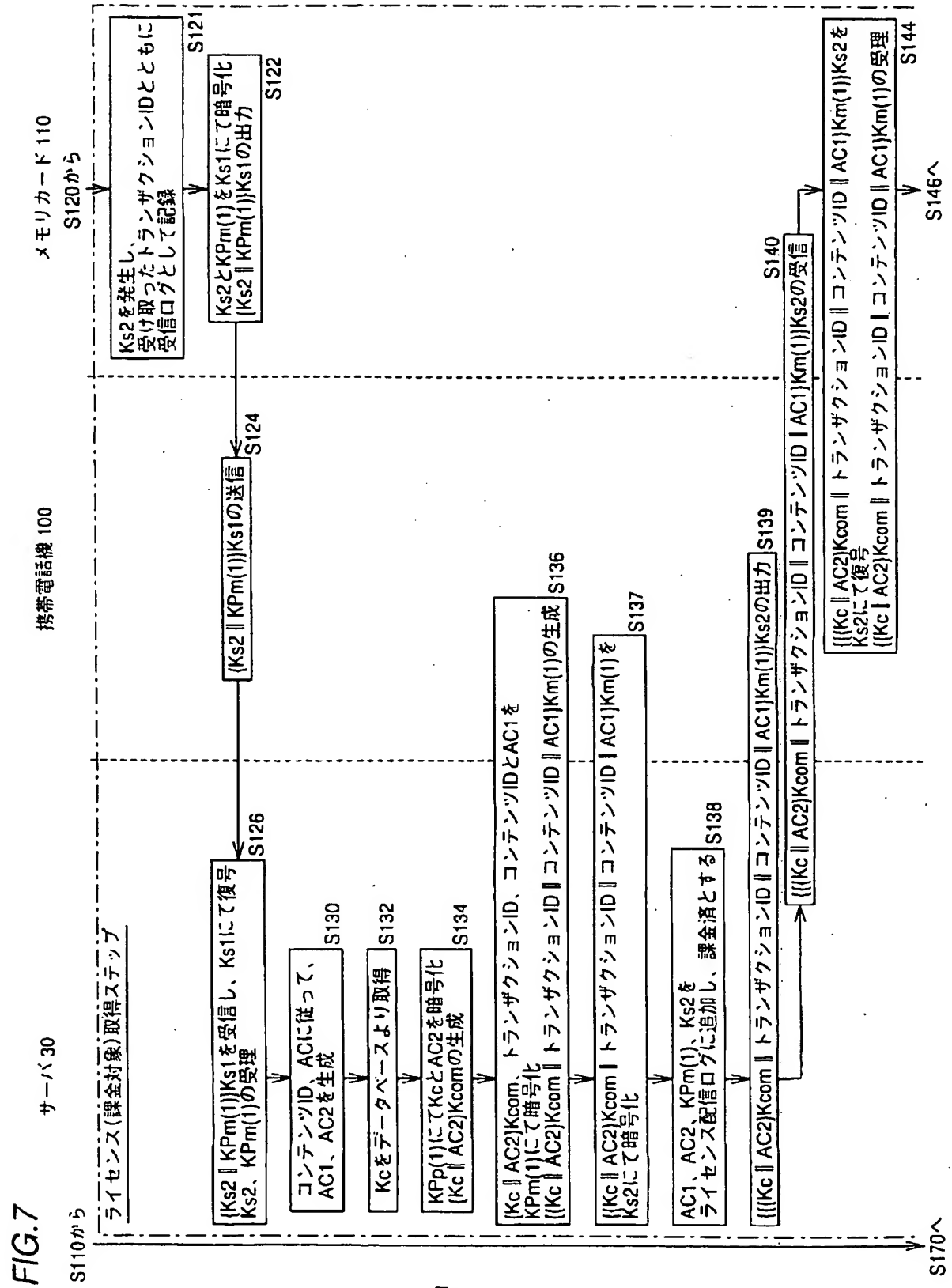
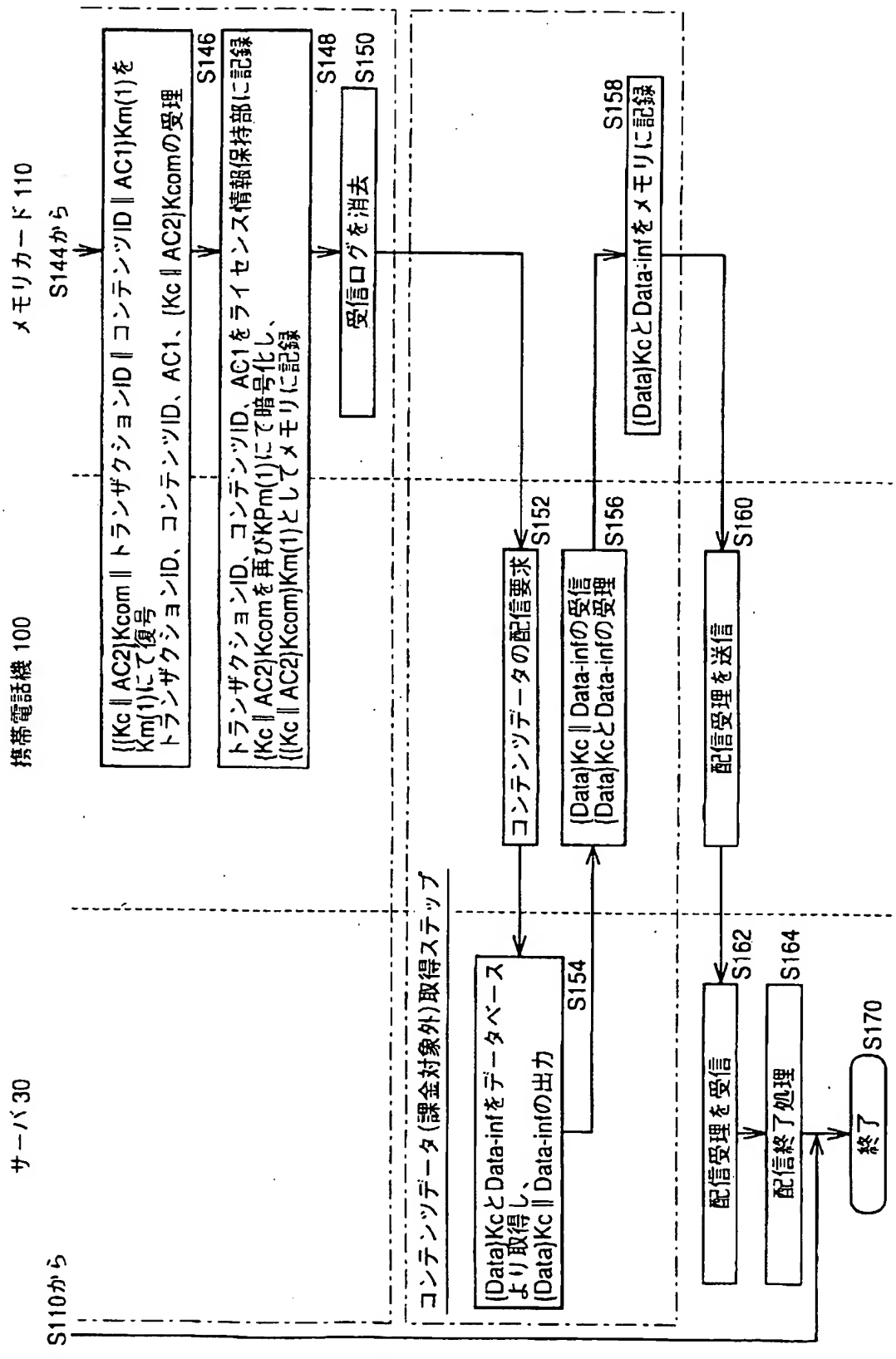

ライセンス(課金対象)取得ステップ
サーバ30
携帯電話機100
メモリカード110
S110から
S120から
S170へ
S146へ
Ks2を発生し、受け取ったトランザクションIDとともに受信ログとして記録
S121
{Ks2 ‖ KPm(1)}Ks1の出力
S122
Ks2とKPm(1)をKs1にて暗号化
{Ks2 ‖ KPm(1)}Ks1の送信
S124
{Ks2 ‖ KPm(1)}Ks1を受信し、Ks1にて復号
Ks2、KPm(1)の受理
S126
コンテンツID、ACに従って、AC1、AC2を生成
S130
Kcをデータベースより取得
S132
KPp(1)にてKcとAC2を暗号化
{Kc ‖ AC2}Kcomの生成
S134
{Kc ‖ AC2}Kcom、トランザクションID、コンテンツIDとAC1を
KPm(1)にて暗号化
{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)の生成
S136
{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)を
Ks2にて暗号化
S137
AC1、AC2、KPm(1)、Ks2を
ライセンス配信ログに追加し、課金済とする
S138
{{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)}Ks2の出力
S139
{{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)}Ks2の受信
S140
{{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)}Ks2を
Ks2にて復号
{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)の受理
S144

FIG.8


S110から
サーバ30
携帯電話機 100
メモリカード 110
S144から
{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)を
Km(1)にて復号
トランザクションID、コンテンツID、AC1、{Kc ‖ AC2}Kcomの受理
S146
トランザクションID、コンテンツID、AC1をライセンス情報保持部に記録
{Kc ‖ AC2}KcomをKPm(1)にて暗号化し、
{{Kc ‖ AC2}Kcom}Km(1)としてメモリに記録
S148
受信ログを消去
S150
コンテンツデータ(課金対象外)取得ステップ
コンテンツデータの配信要求
S152
{Data}KcとData-infをデータベースより取得し、
{Data}Kc ‖ Data-infの出力
S154
{Data}Kc ‖ Data-infの受信
{Data}KcとData-infの受理
S156
{Data}KcとData-infをメモリに記録
S158
配信受理を送信
S160
配信受理を受信
S162
配信終了処理
S164
終了
S170

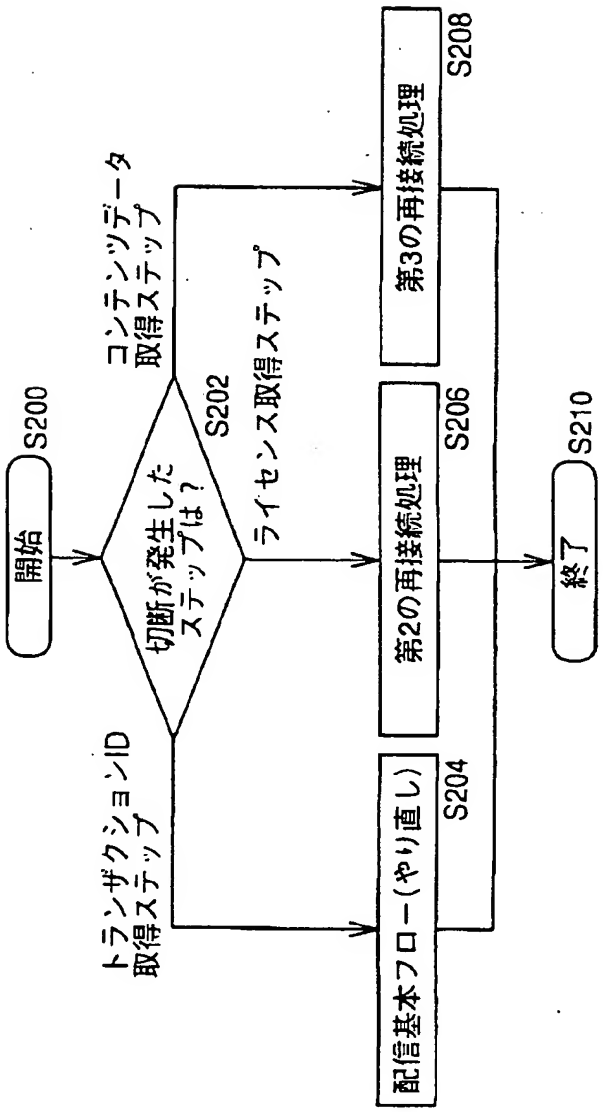

開始
S200
切断が発生したステップは？
S202
トランザクションID取得ステップ
ライセンス取得ステップ
コンテンツデータ取得ステップ
配信基本フロー（やり直し）
S204
第2の再接続処理
S206
第3の再接続処理
S208
終了
S210

FIG.9

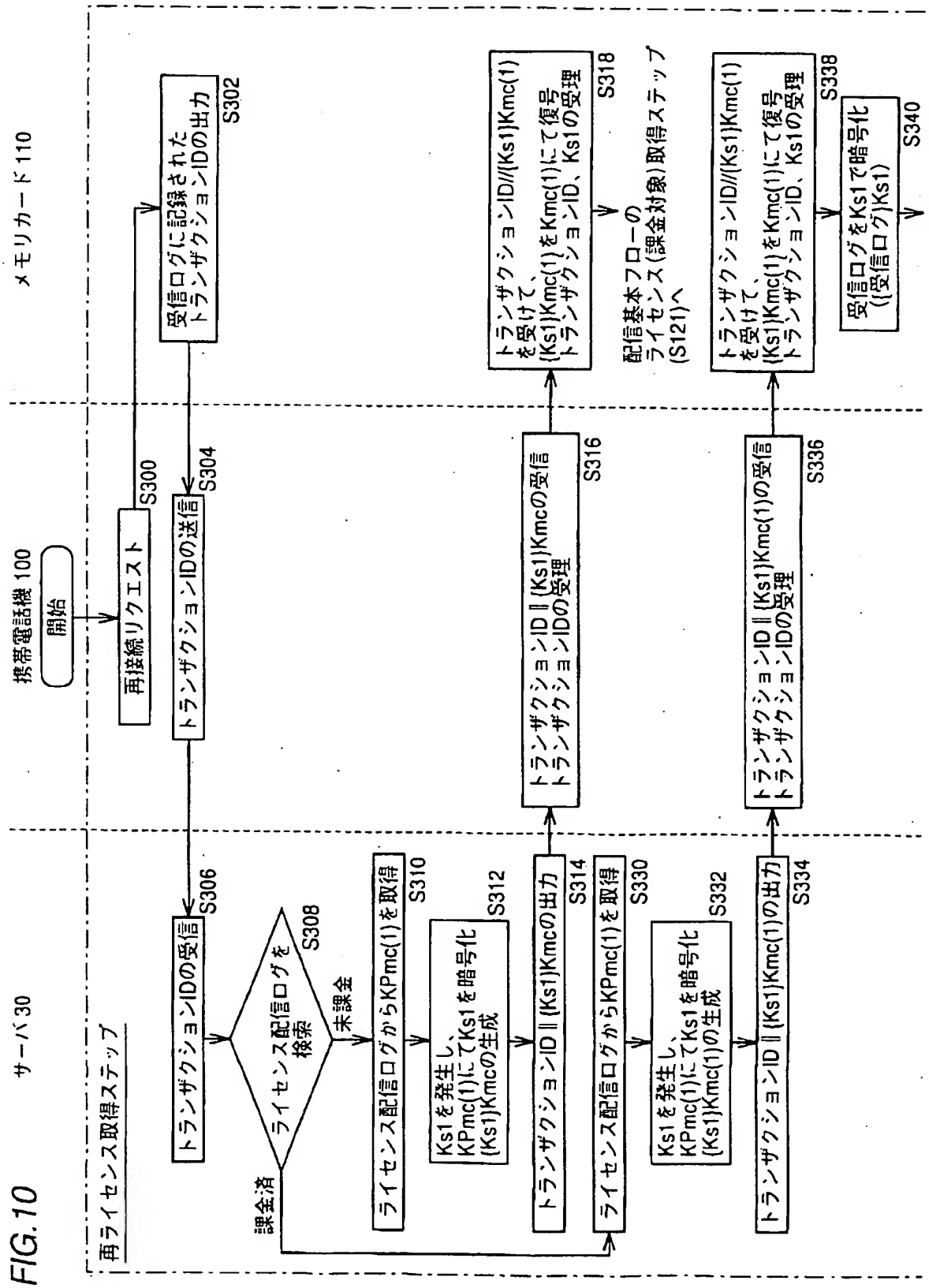

再ライセンス取得ステップ
サーバ30
携帯電話機100
メモリカード110
開始
再接続リクエスト
S300
受信ログに記録されたトランザクションIDの出力
S302
トランザクションIDの送信
S304
トランザクションIDの受信
S306
ライセンス配信ログを検索
S308
課金済
未課金
ライセンス配信ログからKPmc(1)を取得
S310
Ks1を発生し、KPmc(1)にてKs1を暗号化{Ks1}Kmcの生成
S312
トランザクションID‖{Ks1}Kmcの出力
S314
トランザクションID‖{Ks1}Kmcの受信
トランザクションIDの受理
S316
トランザクションID//{Ks1}Kmc(1)を受けて、{Ks1}Kmc(1)をKmc(1)にて復号トランザクションID、Ks1の受理
S318
配信基本フローのライセンス(課金対象)取得ステップ(S121)へ
ライセンス配信ログからKPmc(1)を取得
S330
Ks1を発生し、KPmc(1)にてKs1を暗号化{Ks1}Kmc(1)の生成
S332
トランザクションID‖{Ks1}Kmc(1)の出力
S334
トランザクションID‖{Ks1}Kmc(1)の受信
トランザクションIDの受理
S336
トランザクションID//{Ks1}Kmc(1)を受けて、{Ks1}Kmc(1)をKmc(1)にて復号トランザクションID、Ks1の受理
S338
受信ログをKs1で暗号化({受信ログ}Ks1)
S340
S342へ

FIG.10

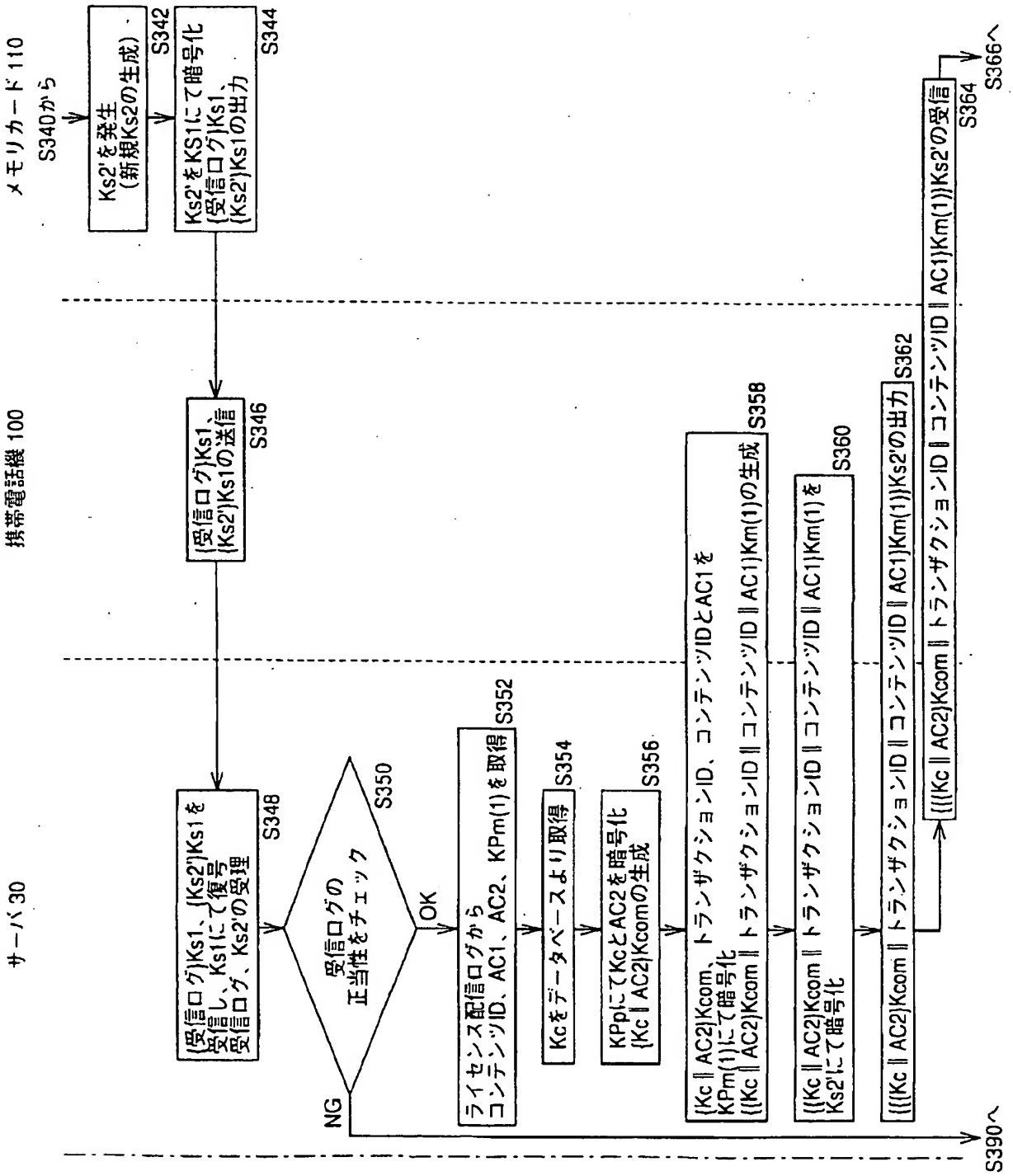

メモリカード 110
携帯電話機 100
サーバ 30
S340から
Ks2'を発生
(新規Ks2の生成)
S342
Ks2'をKS1にて暗号化
{受信ログ}Ks1、
{Ks2'}Ks1の出力
S344
{受信ログ}Ks1、
{Ks2'}Ks1の送信
S346
{受信ログ}Ks1、{Ks2'}Ks1を
受信し、Ks1にて復号
受信ログ、Ks2'の受理
S348
受信ログの
正当性をチェック
S350
NG
OK
ライセンス配信ログから
コンテンツID、AC1、AC2、KPm(1)を取得
S352
Kcをデータベースより取得
S354
KPpにてKcとAC2を暗号化
{Kc || AC2}Kcomの生成
S356
{Kc || AC2}Kcom、トランザクションID、コンテンツIDとAC1を
KPm(1)にて暗号化
{{Kc || AC2}Kcom || トランザクションID || コンテンツID || AC1}Km(1)の生成
S358
{{Kc || AC2}Kcom || トランザクションID || コンテンツID || AC1}Km(1)を
Ks2'にて暗号化
S360
{{{Kc || AC2}Kcom || トランザクションID || コンテンツID || AC1}Km(1)}Ks2'の出力
S362
{{{Kc || AC2}Kcom || トランザクションID || コンテンツID || AC1}Km(1)}Ks2'の受信
S364
S366へ
S390へ

FIG.11

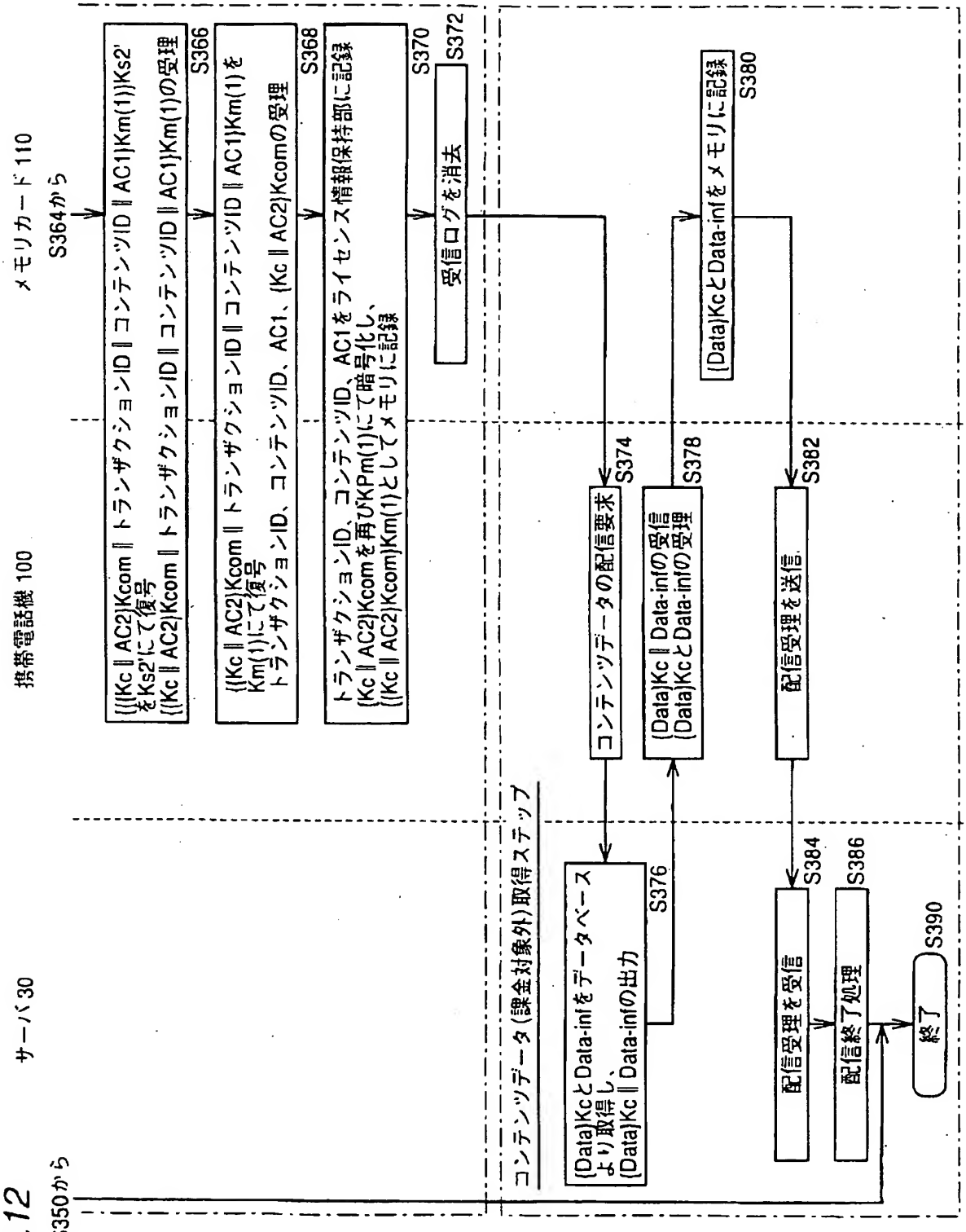

サーバ30
携帯電話機 100
メモリカード 110
S350から
S364から
{{{Kc ‖ AC2)Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1)Km(1)}Ks2'をKs2'にて復号
{(Kc ‖ AC2)Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1)Km(1)の受理
S366
{(Kc ‖ AC2)Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1)Km(1)をKm(1)にて復号
トランザクションID、コンテンツID、AC1、(Kc ‖ AC2)Kcomの受理
S368
トランザクションID、コンテンツID、AC1をライセンス情報保持部に記録
{Kc ‖ AC2)Kcomを再びKPm(1)にて暗号化し、
{(Kc ‖ AC2)Kcom)Km(1)としてメモリに記録
S370
受信ログを消去
S372
コンテンツデータ(課金対象外)取得ステップ
コンテンツデータの配信要求
S374
{Data)Kc ‖ Data-inf)の受信
{Data)KcとData-infの受理
S378
{Data)KcとData-infをメモリに記録
S380
{Data)KcとData-infをデータベースより取得し、
{Data)Kc ‖ Data-infの出力
S376
配信受理を送信
S382
配信受理を受信
S384
配信終了処理
S386
終了
S390

FIG.12

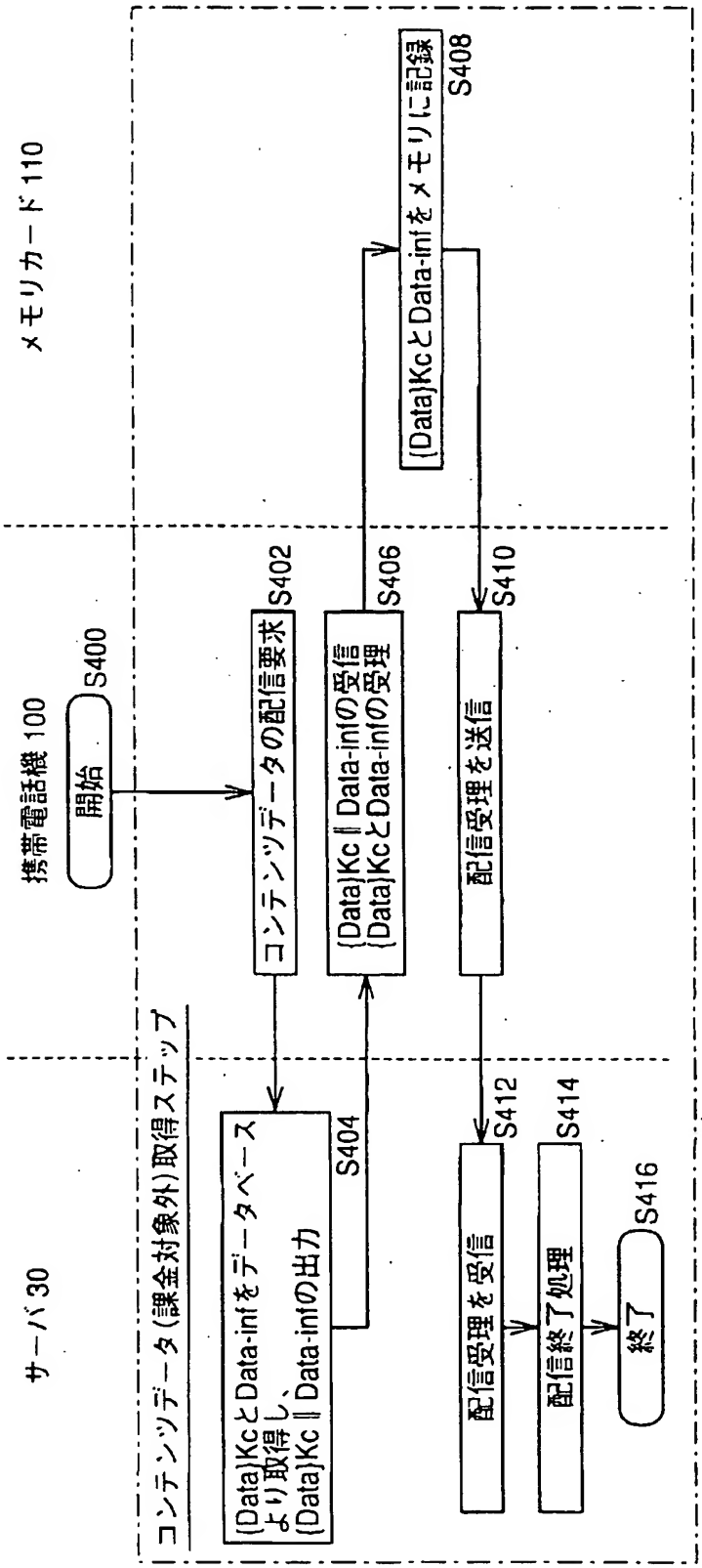

サーバ30
携帯電話機100
メモリカード110
コンテンツデータ(課金対象外)取得ステップ
開始
S400
コンテンツデータの配信要求
S402
{Data}KcとData-infをデータベースより取得し、{Data}Kc‖Data-infの出力
S404
{Data}Kc‖Data-infの受信
{Data}KcとData-infの受理
S406
{Data}KcとData-infをメモリに記録
S408
配信受理を送信
S410
配信受理を受信
S412
配信終了処理
S414
終了
S416

FIG.13

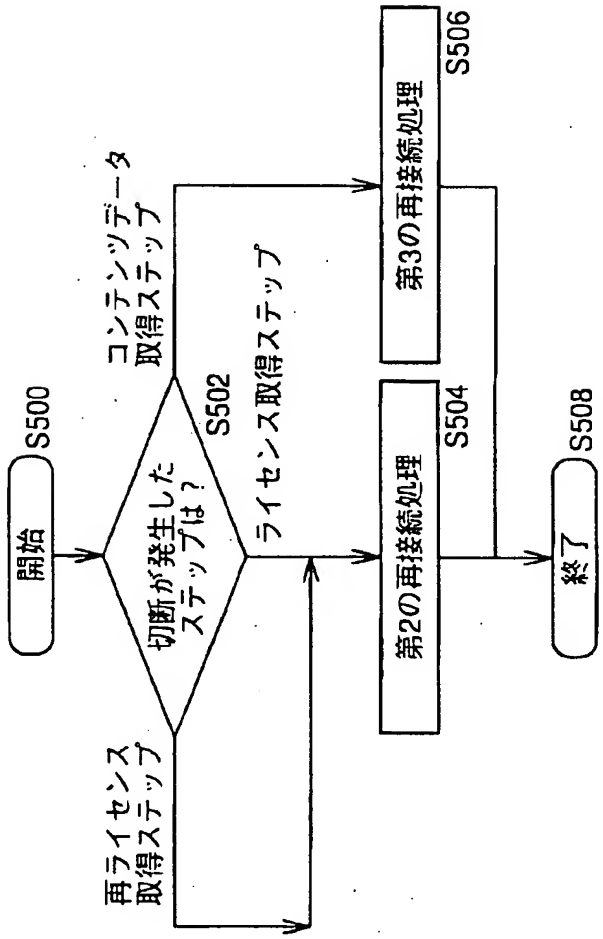

開始
S500
切断が発生したステップは？
S502
コンテンツデータ取得ステップ
ライセンス取得ステップ
再ライセンス取得ステップ
第3の再接続処理
S506
第2の再接続処理
S504
終了
S508

FIG.14

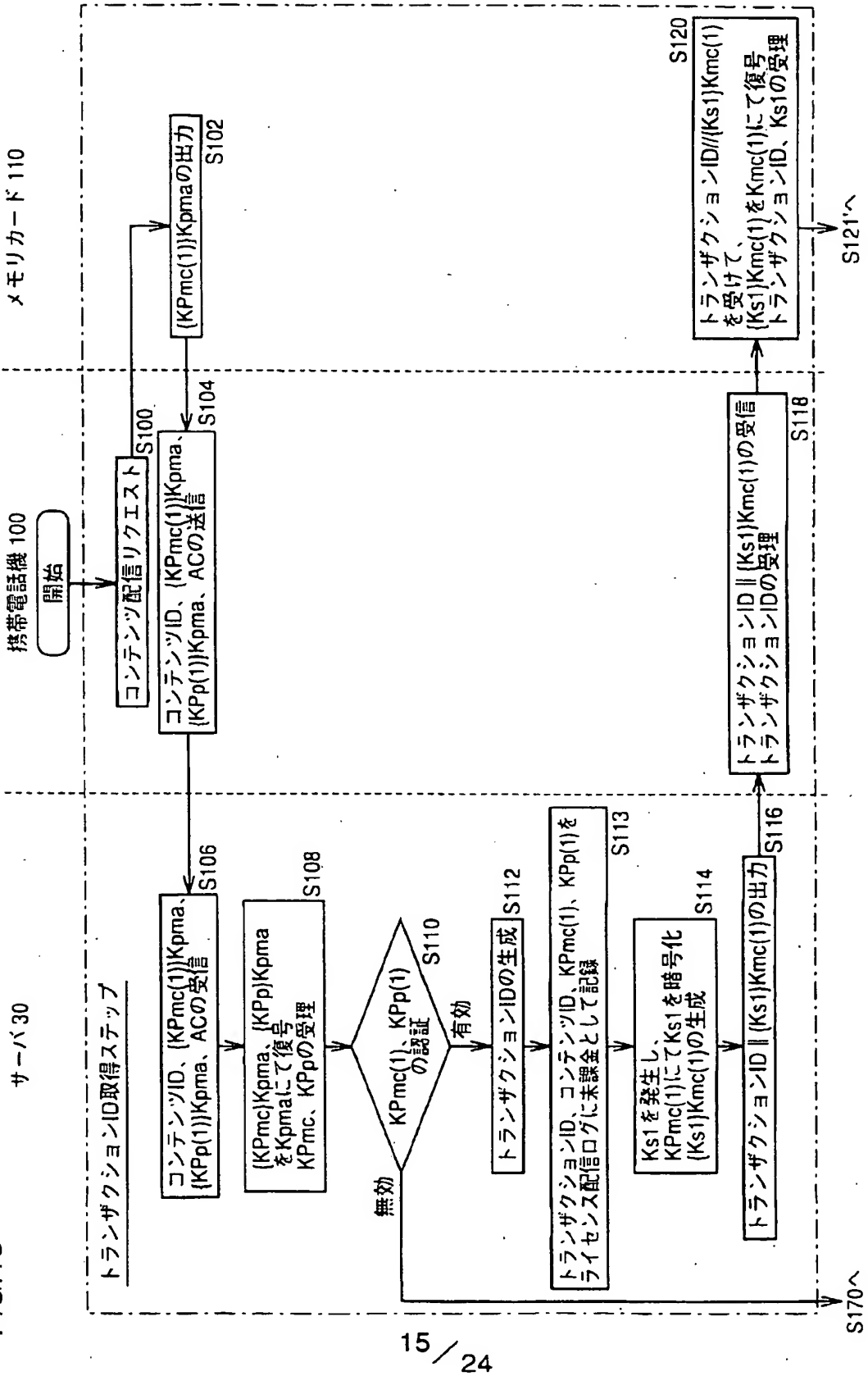

携帯電話機 100
メモリカード 110
サーバ 30
トランザクションID取得ステップ
開始
コンテンツ配信リクエスト
S100
{KPmc(1)}Kpmaの出力
S102
コンテンツID、{KPmc(1)}Kpma、{KPp(1)}Kpma、ACの送信
S104
コンテンツID、{KPmc(1)}Kpma、{KPp(1)}Kpma、ACの受信
S106
{KPmc}Kpmaを{KPp}Kpmaにて復号
KPmc、KPpの受理
S108
KPmc(1)、KPp(1)の認証
S110
無効
有効
トランザクションIDの生成
S112
トランザクションID、コンテンツID、KPmc(1)、KPp(1)をライセンス配信ログに未課金として記録
S113
Ks1を発生し、KPmc(1)にてKs1を暗号化{Ks1}Kmc(1)の生成
S114
トランザクションID‖{Ks1}Kmc(1)の出力
S116
トランザクションID‖{Ks1}Kmc(1)の受信
トランザクションIDの受理
S118
トランザクションID//{Ks1}Kmc(1)を受けて、
{Ks1}Kmc(1)を{Kmc(1)にて復号
トランザクションID、Ks1の受理
S120
S121'へ
S170へ

FIG.15

FIG.16

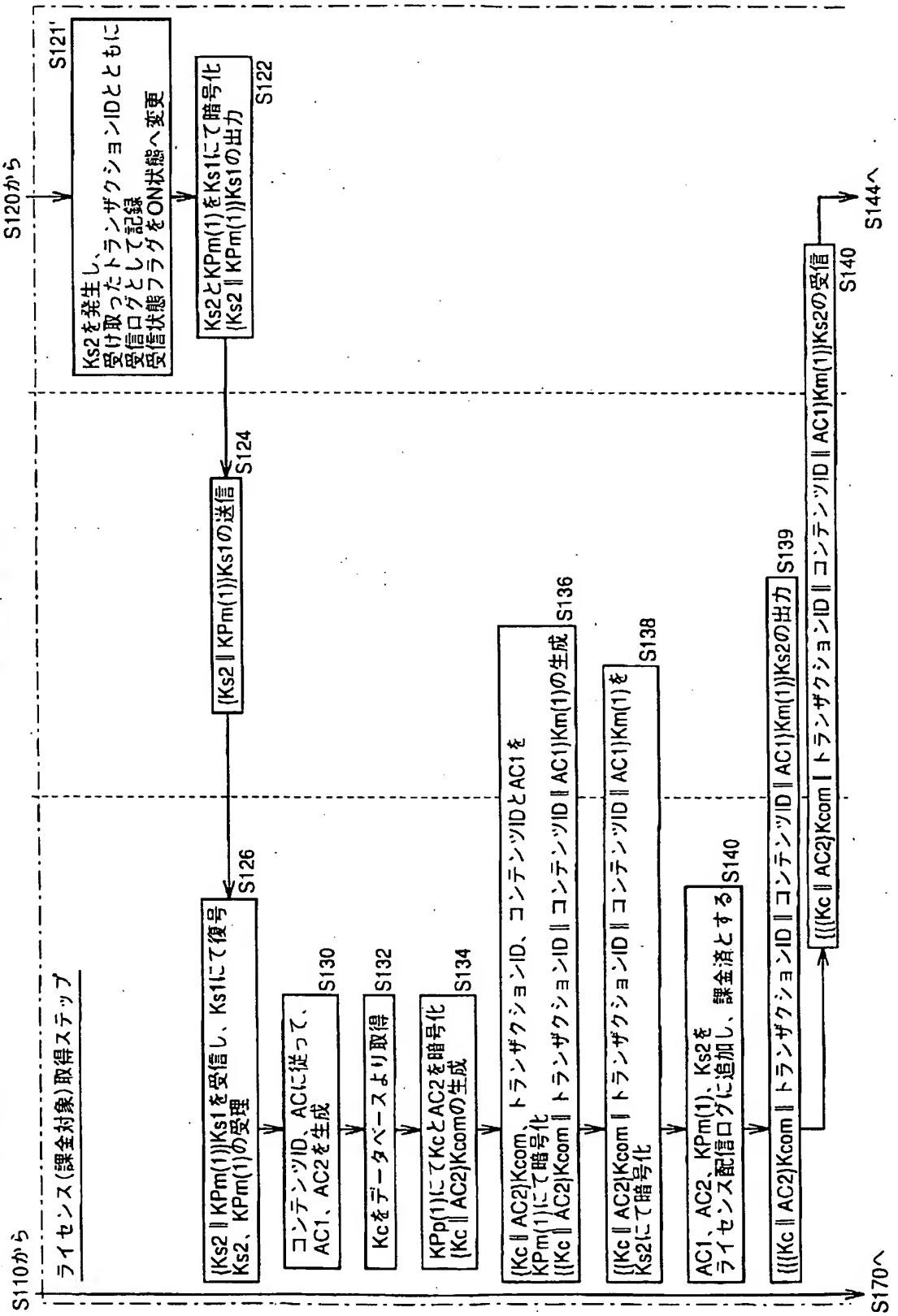

サーバ 30
携帯電話機 100
メモリカード 110
S110から
ライセンス(課金対象)取得ステップ
S120から
S121'
Ks2を発生し、
受け取ったトランザクションIDとともに
受信ログとして記録
受信状態フラグをON状態へ変更
S122
Ks2とKPm(1)をKs1にて暗号化
{Ks2 ‖ KPm(1)}Ks1の出力
S124
{Ks2 ‖ KPm(1)}Ks1の送信
S126
{Ks2 ‖ KPm(1)}Ks1を受信し、Ks1にて復号
Ks2、KPm(1)の受理
S130
コンテンツID、ACに従って、
AC1、AC2を生成
S132
Kcをデータベースより取得
S134
KPp(1)にてKcとAC2を暗号化
{Kc ‖ AC2}Kcomの生成
S136
{Kc ‖ AC2}Kcom、トランザクションID、コンテンツIDとAC1を
KPm(1)にて暗号化
{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)の生成
S138
{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)を
Ks2にて暗号化
S140
AC1、AC2、KPm(1)、Ks2を
ライセンス配信ログに追加し、課金済とする
S139
{{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)}Ks2の出力
S140
{{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)}Ks2の受信
S144へ
S170へ

FIG. 17

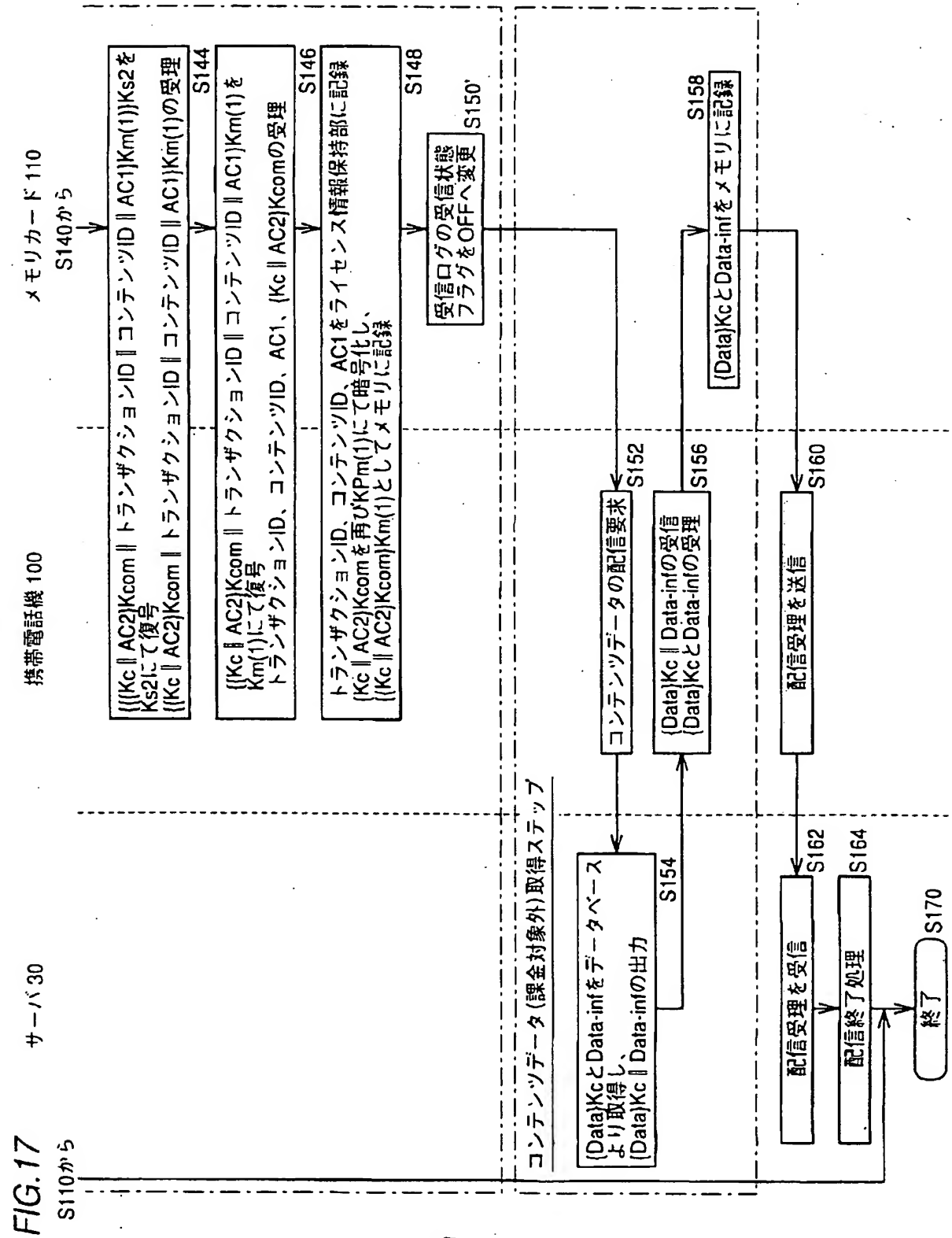
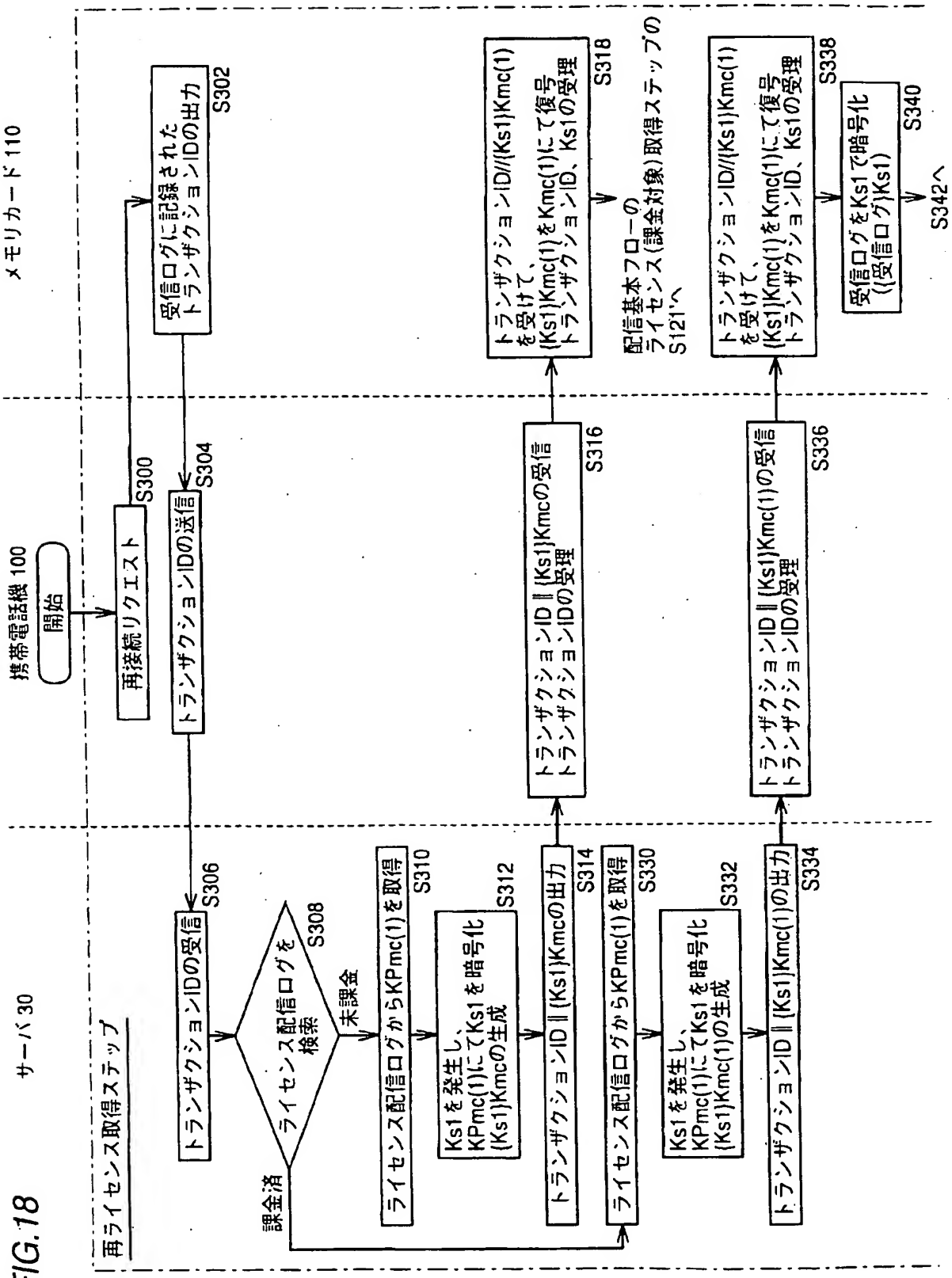

S110から
サーバ30
携帯電話機100
メモリカード110
S140から
{{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)}Ks2を
Ks2にて復号
{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)の受理
S144
{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)を
Km(1)にて復号
トランザクションID、コンテンツID、AC1、{Kc ‖ AC2}Kcomの受理
S146
トランザクションID、コンテンツID、AC1をライセンス情報保持部に記録
{Kc ‖ AC2}Kcomを再びKPm(1)にて暗号化し、
{{Kc ‖ AC2}Kcom}Km(1)としてメモリに記録
S148
受信ログの受信状態
フラグをOFFへ変更
S150'
コンテンツデータ(課金対象外)取得ステップ
コンテンツデータの配信要求
S152
{Data}Kc ‖ Data-infの受信
{Data}KcとData-infの受理
S156
{Data}KcとData-infをメモリに記録
S158
配信受理を送信
S160
{Data}KcとData-infをデータベース
より取得し、
{Data}Kc ‖ Data-infの出力
S154
配信受理を受信
S162
配信終了処理
S164
終了
S170

FIG.18


再ライセンス取得ステップ
携帯電話機 100
サーバ 30
メモリカード 110
開始
再接続リクエスト
S300
受信ログに記録されたトランザクションIDの出力
S302
トランザクションIDの送信
S304
トランザクションIDの受信
S306
ライセンス配信ログを検索
S308
課金済
未課金
ライセンス配信ログからKPmc(1)を取得
S310
Ks1を発生し、KPmc(1)にてKs1を暗号化(Ks1)Kmcの生成
S312
トランザクションID‖(Ks1)Kmcの出力
S314
トランザクションID‖(Ks1)Kmcの受信トランザクションIDの受理
S316
トランザクションID//(Ks1)Kmc(1)を受けて、(Ks1)Kmc(1)をKmc(1)にて復号トランザクションID、Ks1の受理
S318
配信基本フローのライセンス(課金対象)取得ステップのS121'へ
ライセンス配信ログからKPmc(1)を取得
S330
Ks1を発生し、KPmc(1)にてKs1を暗号化(Ks1)Kmc(1)の生成
S332
トランザクションID‖(Ks1)Kmc(1)の出力
S334
トランザクションID‖(Ks1)Kmc(1)の受信トランザクションIDの受理
S336
トランザクションID//(Ks1)Kmc(1)を受けて、(Ks1)Kmc(1)をKmc(1)にて復号トランザクションID、Ks1の受理
S338
受信ログをKs1で暗号化(受信ログ)(Ks1)
S340
S342へ

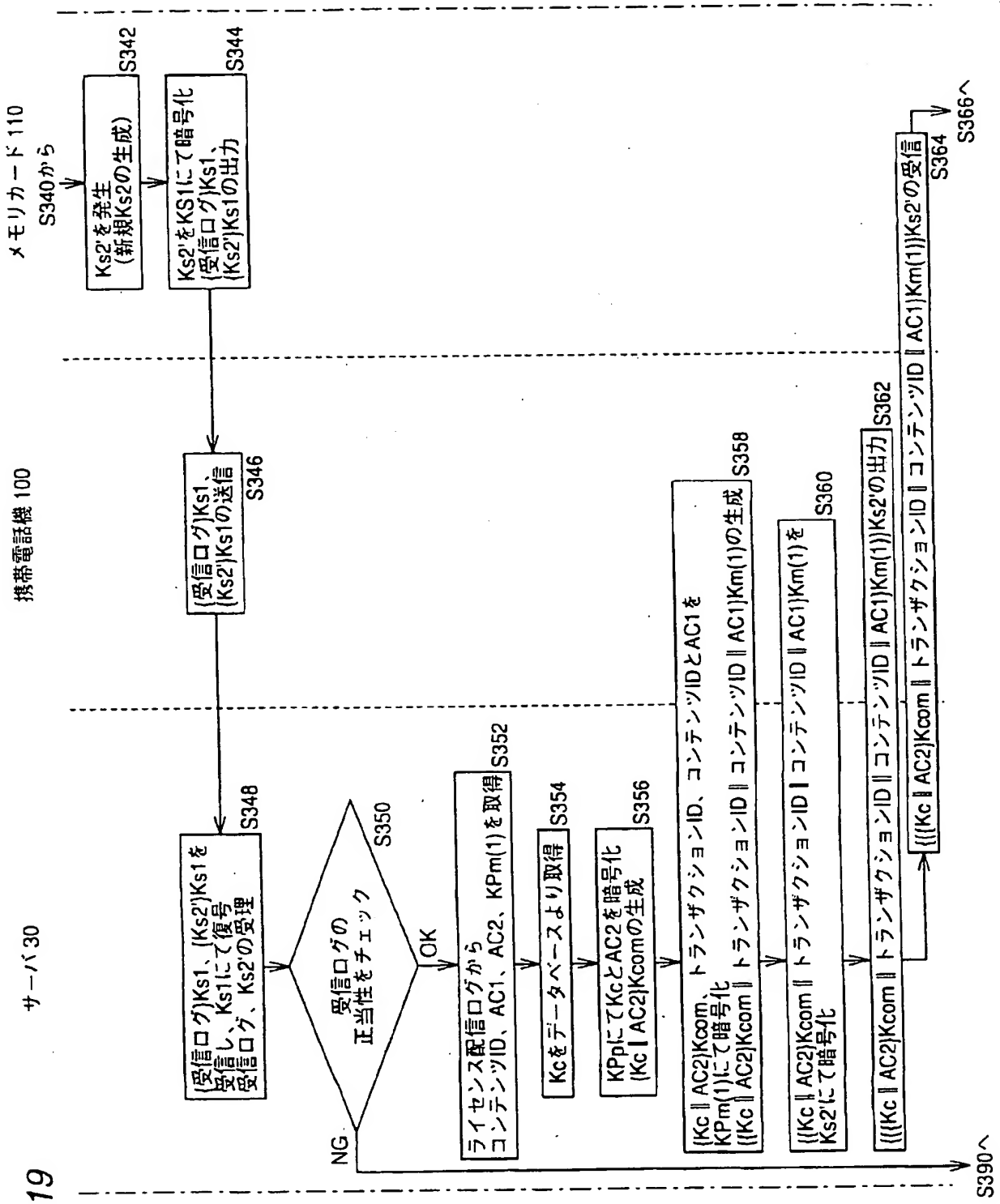

メモリカード 110
携帯電話機 100
サーバ 30
S340から
Ks2'を発生
(新規Ks2の生成)
S342
Ks2'をKS1にて暗号化
{受信ログ}Ks1、
{Ks2'}Ks1の出力
S344
{受信ログ}Ks1、
{Ks2'}Ks1の送信
S346
{受信ログ}Ks1、{Ks2'}Ks1を
受信し、Ks1にて復号
受信ログ、Ks2'の受理
S348
受信ログの
正当性をチェック
S350
NG
OK
ライセンス配信ログから
コンテンツID、AC1、AC2、KPm(1)を取得
S352
Kcをデータベースより取得
S354
KPpにてKcとAC2を暗号化
{Kc ‖ AC2}Kcomの生成
S356
{Kc ‖ AC2}Kcom、トランザクションID、コンテンツIDとAC1を
KPm(1)にて暗号化
{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)の生成
S358
{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)を
Ks2'にて暗号化
S360
{{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)}Ks2'の出力
S362
{{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)}Ks2'の受信
S364
S366へ
S390へ

FIG.19

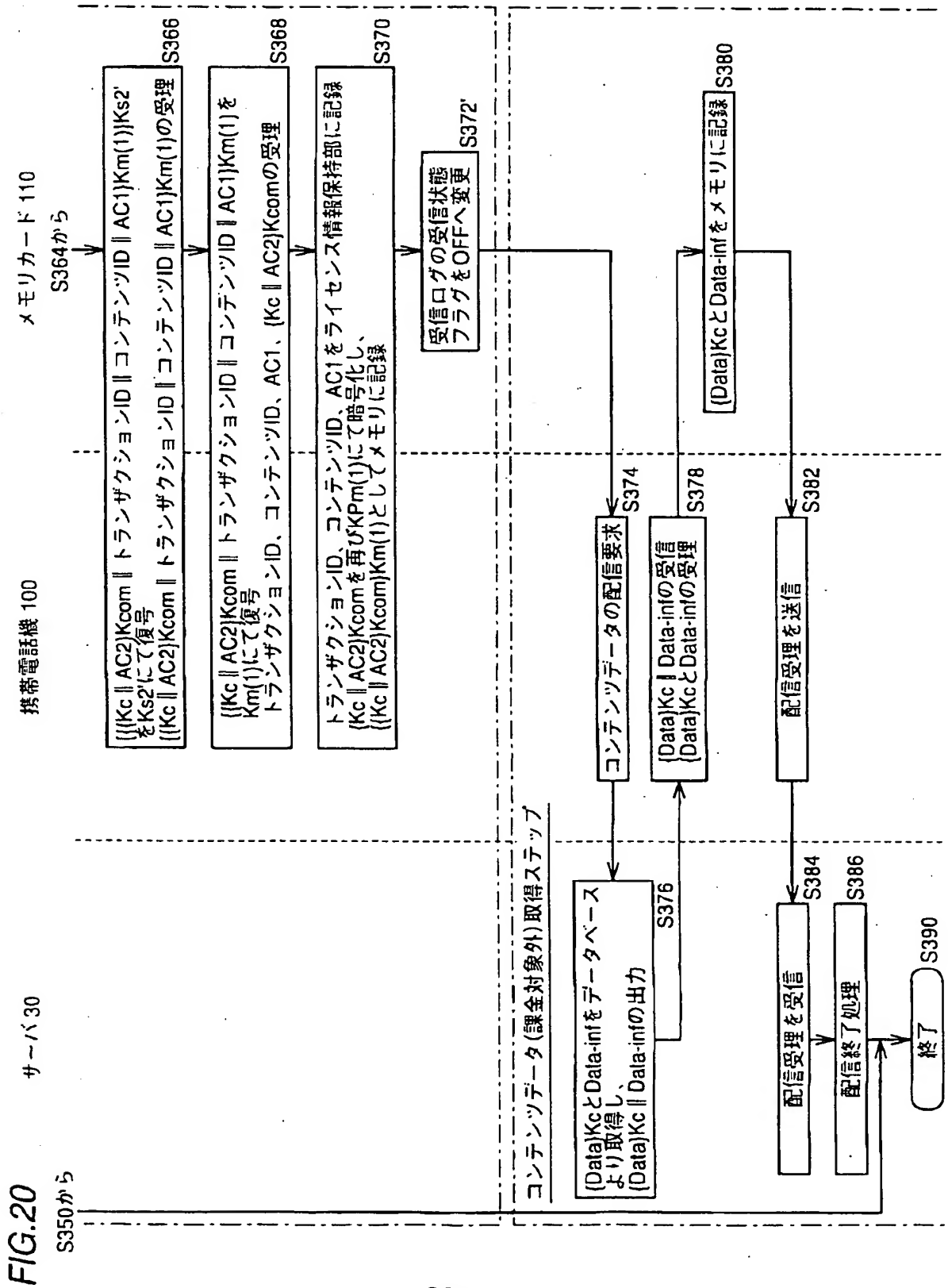

携帯電話機 100
メモリカード 110
サーバ 30
S350から
S364から
{{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)}Ks2'
をKs2'にて復号
{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)の受理
S366
{{Kc ‖ AC2}Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1}Km(1)を
Km(1)にて復号
トランザクションID、コンテンツID、AC1、{Kc ‖ AC2}Kcomの受理
S368
トランザクションID、コンテンツID、AC1をライセンス情報保持部に記録
{Kc ‖ AC2}KcomをKPm(1)にて暗号化し、
{{Kc ‖ AC2}Kcom}Km(1)としてメモリに記録
S370
受信ログの受信状態
フラグをOFFへ変更
S372'
コンテンツデータ(課金対象外)取得ステップ
コンテンツデータの配信要求
S374
{Data}KcとData-infをデータベース
より取得し、
{Data}Kc ‖ Data-infの出力
S376
{Data}Kc ‖ Data-infの受信
{Data}KcとData-infの受理
S378
{Data}KcとData-infをメモリに記録
S380
配信受理を送信
S382
配信受理を受信
S384
配信終了処理
S386
終了
S390

FIG.20

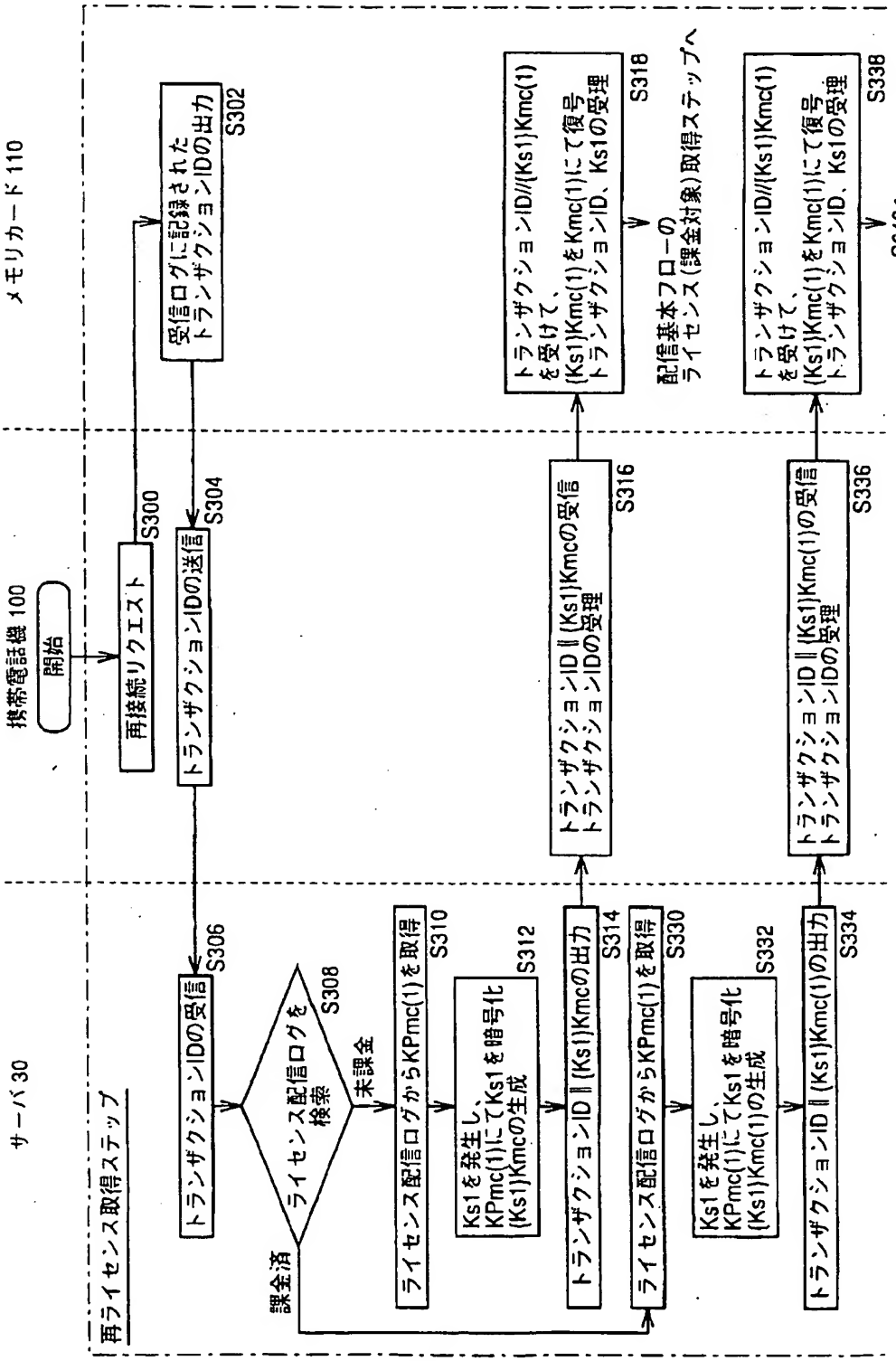

再ライセンス取得ステップ
サーバ30
携帯電話機100
メモリカード110
開始
再接続リクエスト
S300
受信ログに記録された
トランザクションIDの出力
S302
トランザクションIDの送信
S304
トランザクションIDの受信
S306
ライセンス配信ログを
検索
S308
課金済
未課金
ライセンス配信ログからKPmc(1)を取得
S310
Ks1を発生し、
KPmc(1)にてKs1を暗号化
(Ks1)Kmcの生成
S312
トランザクションID‖(Ks1)Kmcの出力
S314
トランザクションID‖(Ks1)Kmcの受信
トランザクションIDの受理
S316
トランザクションID//(Ks1)Kmc(1)
を受けて、
(Ks1)Kmc(1)をKmc(1)にて復号
トランザクションID、Ks1の受理
S318
配信基本フローの
ライセンス(課金対象)取得ステップへ
ライセンス配信ログからKPmc(1)を取得
S330
Ks1を発生し、
KPmc(1)にてKs1を暗号化
(Ks1)Kmc(1)の生成
S332
トランザクションID‖(Ks1)Kmc(1)の出力
S334
トランザクションID‖(Ks1)Kmc(1)の受信
トランザクションIDの受理
S336
トランザクションID//(Ks1)Kmc(1)
を受けて、
(Ks1)Kmc(1)をKmc(1)にて復号
トランザクションID、Ks1の受理
S338
S640へ

FIG.21

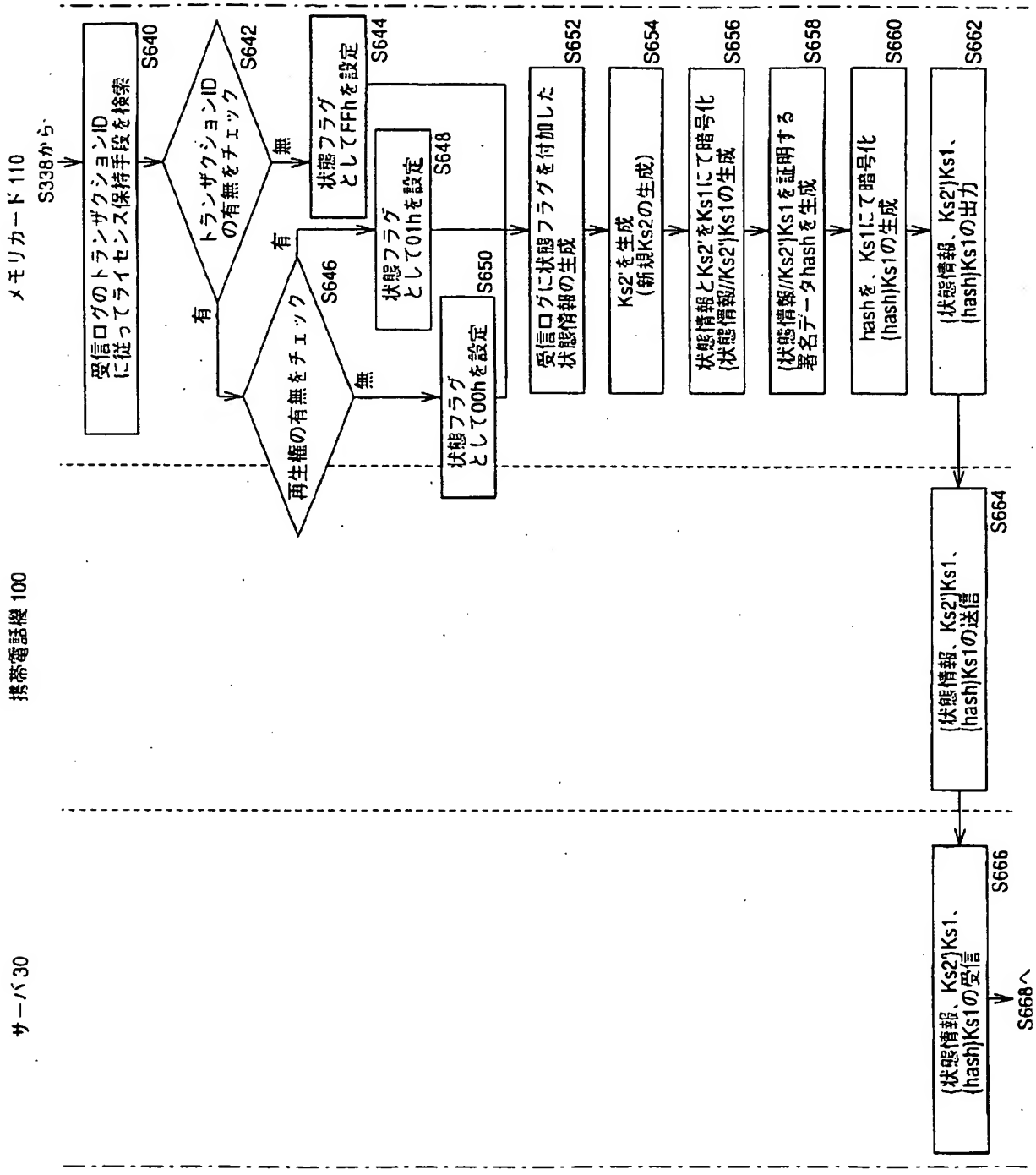

メモリカード 110
携帯電話機 100
サーバ 30
S338から
受信ログのトランザクションID
に従ってライセンス保持手段を検索
S640
トランザクションID
の有無をチェック
S642
有
無
状態フラグ
としてFFhを設定
S644
再生権の有無をチェック
S646
有
無
状態フラグ
として01hを設定
S648
状態フラグ
として00hを設定
S650
受信ログに状態フラグを付加した
状態情報の生成
S652
Ks2'を生成
(新規Ks2の生成)
S654
状態情報とKs2'をKs1にて暗号化
{状態情報//Ks2'}Ks1の生成
S656
{状態情報//Ks2'}Ks1を証明する
署名データhashを生成
S658
hashを、Ks1にて暗号化
{hash}Ks1の生成
S660
{状態情報、Ks2'}Ks1、
{hash}Ks1の出力
S662
{状態情報、Ks2'}Ks1、
{hash}Ks1の送信
S664
{状態情報、Ks2'}Ks1、
{hash}Ks1の受信
S666
S668へ

FIG.22

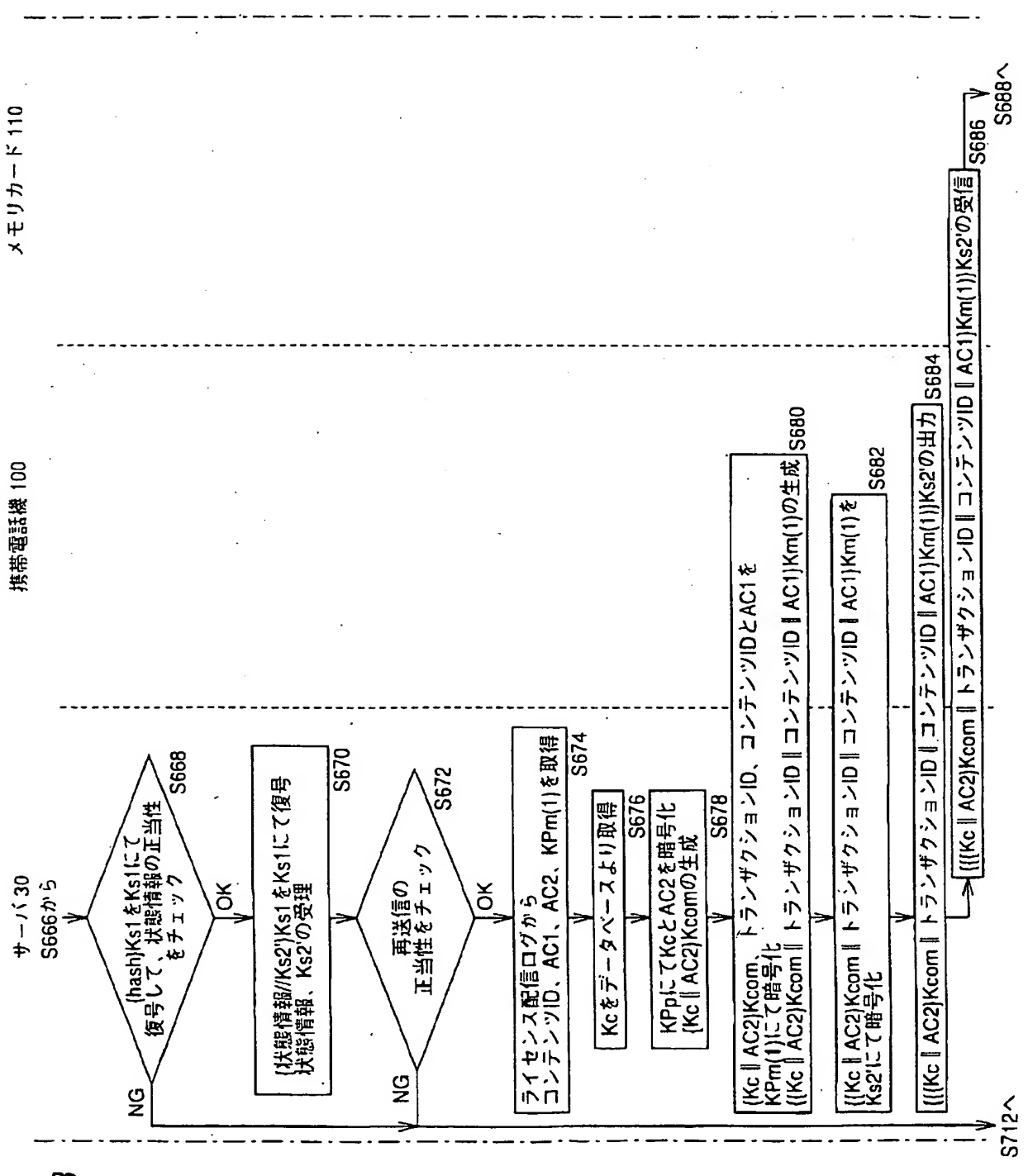

メモリカード110
携帯電話機100
サーバ30
S666から
{hash)Ks1をKs1にて復号して、状態情報の正当性をチェック
S668
NG
OK
{状態情報//Ks2')Ks1をKs1にて復号
状態情報、Ks2'の受理
S670
再送信の正当性をチェック
S672
NG
OK
ライセンス配信ログからコンテンツID、AC1、AC2、KPm(1)を取得
S674
Kcをデータベースより取得
S676
KPpにてKcとAC2を暗号化
{Kc ‖ AC2)Kcomの生成
S678
{Kc ‖ AC2)Kcom、トランザクションID、コンテンツIDとAC1をKPm(1)にて暗号化
{(Kc ‖ AC2)Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1)Km(1)の生成
S680
{(Kc ‖ AC2)Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1)Km(1)をKs2'にて暗号化
S682
{{(Kc ‖ AC2)Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1)Km(1)}Ks2'の出力
S684
{{{(Kc ‖ AC2)Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1)Km(1)}Ks2'の受信
S686
S688へ
S712へ

FIG.23

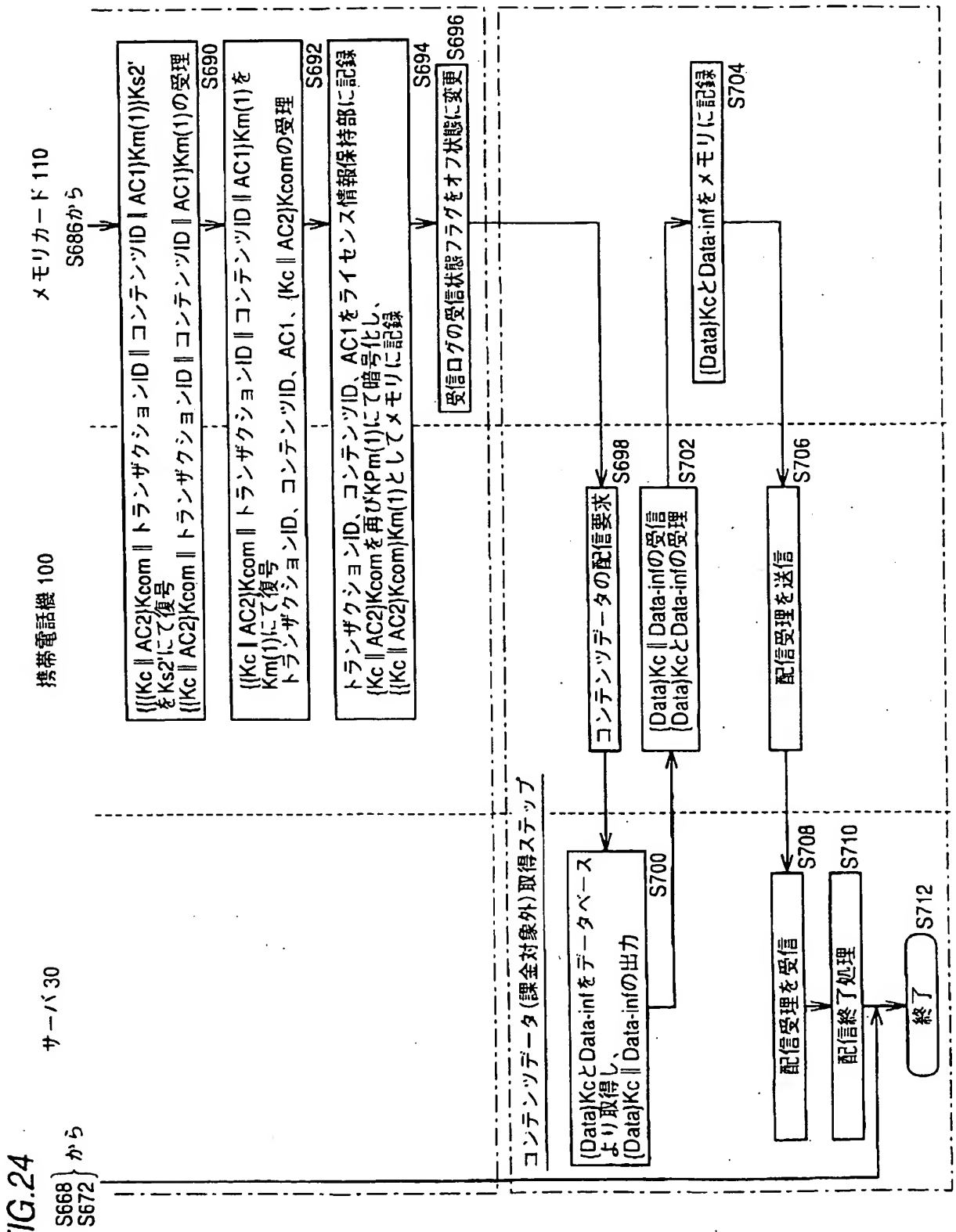

S668
S672
から
サーバ30
携帯電話機100
メモリカード110
S686から
{{{Kc ‖ AC2)Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1)Km(1)}Ks2'
をKs2'にて復号
{{Kc ‖ AC2)Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1)Km(1)の受理
S690
{{Kc ‖ AC2)Kcom ‖ トランザクションID ‖ コンテンツID ‖ AC1)Km(1)を
Km(1)にて復号
トランザクションID、コンテンツID、AC1、{Kc ‖ AC2)Kcomの受理
S692
トランザクションID、コンテンツID、AC1をライセンス情報保持部に記録
{Kc ‖ AC2)Kcomを再びKPm(1)にて暗号化し、
{{Kc ‖ AC2)Kcom)Km(1)としてメモリに記録
S694
受信ログの受信状態フラグをオフ状態に変更
S696
コンテンツデータ(課金対象外)取得ステップ
{Data)KcとData-infをデータベースより取得し、
{Data)Kc ‖ Data-infの出力
S700
コンテンツデータの配信要求
S698
{Data)Kc ‖ Data-infの受信
{Data)KcとData-infの受理
S702
{Data)KcとData-infをメモリに記録
S704
配信受理を送信
S706
配信受理を受信
S708
配信終了処理
S710
終了
S712

FIG.24

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/08544

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L 9/10 G06F 12/14, G10K 15/02 G06F 13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L 9/00 H04K 1/00-3/00 G09C 1/00-5/00
G06F 12/00-13/00 G10K 15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS)
WPI(DIALOG)
INSPEC(DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 11-224288, A (Hitachi, Ltd.), 17 August, 1999 (17.08.99) & EP, 935209, A2 & SG, 75914, A1 & CA, 2260536, A1	1-17
EA	JP, 2000-253453, A (Sony Corporation), 14 September, 2000 (14.09.00) & EP, 1033894, A2 & CN, 1266326, A	1-17
EA	JP, 2000-268096, A (Dainippon Printing Co., Ltd.), 29 September, 2000 (29.09.00) (Family: none)	1-17

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
08 March, 2001 (08.03.01)

Date of mailing of the international search report
21 March, 2001 (21.03.01)

Name and mailing address of the ISA/
Japanese Patent Office

Facsimile No.

Authorized officer

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　PCT／JP00／08544

A.　発明の属する分野の分類（国際特許分類（IPC））
Int. Cl⁷
H04L 9／10　G06F 12／14,　G10K 15／02　G06F 13／00

B.　調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
Int. Cl⁷
H04L 9／00　H04K 1／00－3／00　G09C 1／00－5／00
G06F 12／00－13／00　G10K 15／00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2001年
日本国登録実用新案公報　1994－2001年
日本国実用新案登録公報　1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
JICSTファイル（JOIS）
WPI（DIALOG）
INSPEC（DIALOG）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP, 11－224288, A（株式会社日立製作所） 17. 8月. 1999（17. 08. 99） & EP, 935209, A2 & SG, 75914, A1 & CA, 2260536, A1	1-17
EA	JP, 2000－253453, A（ソニー株式会社） 14. 9月. 2000（14. 09. 00） & EP, 1033894, A2 & CN, 1266326, A	1-17

☑ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 08. 03. 01	国際調査報告の発送日　21.03.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 丸山　高政　印　5W　9570 電話番号　03－3581－1101　内線　3574

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　PCT／JP00／08544

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
EA	JP，2000－268096，A（大日本印刷株式会社） 29．9月．2000（29．09．00）， （ファミリーなし）	1-17

様式PCT／ISA／210（第2ページの続き）（1998年7月）